ON THE ENERGY VARIANT OF THE SUM-PRODUCT CONJECTURE

MISHA RUDNEV, ILYA D. SHKREDOV, AND SOPHIE STEVENS

Abstract. We prove new exponents for the energy version of the Erdős-Szemerédi sum-product conjecture, raised by Balog and Wooley. They match the previously established milestone values for the standard formulation of the question, both for general fields and the special case of real or complex numbers, and appear to be the best ones attainable within the currently available technology. Further results are obtained about multiplicative energies of additive shifts and a strengthened energy version of the “few sums, many products” inequality of Elekes and Ruzsa. The latter inequality enables us to obtain a minor improvement of the state-of-the-art sum-product exponent over the reals due to Konyagin and the second author, up to $\frac{5}{4} + \frac{1}{1509}$. An application of energy estimates to an instance of arithmetic growth in prime residue fields is presented.

1. Preface

In this paper we show that the milestone results in the current sum-product theory literature allow for a pure energy formulation involving both addition and multiplication. Previous inequalities of sum-product type involve either $|A \cdot A|$ and $|A + A|$, or $E^+(A)$ and $|A \cdot A|$, or $E^+(A)$ and $|A + A|$. The energy-energy formulation was raised by Balog and Wooley [2]; its key feature being that the sum-product conjecture cannot hold in its maximum strength in the energy formulation. Owing to an example in [2], which we will shortly retell, the cardinality formulation as Conjecture 1 below should be weakened to the energy version as Conjecture 2. The latter suggests a somewhat uncomfortably-looking fractional exponent.

We advance largely on the technical level. The well-established tool in additive combinatorics for passing from energy-type results to the existence of subsets with the desired structure is the Balog-Szemerédi-Gowers theorem. This has been done, in particular, by Balog and Wooley, as well as much earlier work on the relation between geometric incidences and algebraic growth, such as [6], [13]. But for someone concerned with quantitative values of the resulting exponents, the use of the Balog-Szemrerédi-Gowers theorem usually comes at a price.

It was first observed that the Balog-Szemerédi-Gowers theorem can be avoided by Konyagin and the second author [17] who succeeded in significantly strengthening the main estimate of [2]. But the final exponent in the resulting energy-energy inequality in [17] has nonetheless stopped short of its cardinality-cardinality predecessor due to Elekes [8].

2000 Mathematics Subject Classification. 68R05,11B75.
In this paper we remove this gap and prove a variety of energy-energy sum-product type inequalities, which have the same exponents as their cardinality prototypes, up to logarithmic factors. The first of our key inequalities dealing with real/complex numbers is (7), which is the energy-energy analogue of the classical sum-product $5/4$ result by Elekes [8], which we record here as (2). The two energies appearing in this inequality can be replaced by energies of two different additive shifts of a set (which is useful for applications), see Theorem 9. The second inequality is given by (10), which, in a certain sharp regime, is the energy version of the “few sums, many products” inequality by Elekes and Ruzsa [9]. As a matter of fact (10) has better exponents than its prototype, see the discussion before the formulation of the corresponding Theorem 12.

We also furnish the general field variants of our energy inequalities, valid in particular in positive characteristic, with an inevitable constraint on how small the set in question should be. They are usually just slightly weaker than for the particular case of the real or complex field. This combines the pruning techniques developed in this paper with the use of the incidence theorem of the first author from [21] and its further development in [20], [1].

We strongly feel (although we make no attempt to substantiate this claim), that these energy exponents are the best ones attainable within the currently available technology. For the real or complex field there are better sum-product exponents, based on the foundational work by Solymosi [27], [28]. But these appear to necessarily involve cardinality of at least one counterpart, rather than the two energies. For general fields, there are no better ones so far. It appears that further significant progress towards the sum-product conjecture challenges one to break these energy barriers.

Finally, in the main body of the paper we discuss some applications of our energy-energy sum-product type inequalities: some in passing and one at length.

2. Introduction and main results

Let $\mathbb{F}$ be a field, with the multiplicative group $\mathbb{F}^*$ and let $A \subset \mathbb{F}$ be a finite set. The sum set, product set and quotient set of $A$ are defined respectively as

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

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

$$A/A := \{a/b : a, b \in A, b \neq 0\}.$$ 

Sum, etc. sets involving different sets, say $A + B$ are defined in a similar way. For $x \in \mathbb{F}^*$, we write simply $xA$ for $\{x\}A$ and $x + A$ or $A + x$ for $\{x\} + A$.

It has long been observed that unless $A$ is in some sense close to a coset of a subfield of $\mathbb{F}$, additive and multiplicative structure find it hard to coexist: it is easy to minimise one of $|A + A|$ or $|A \cdot A|$ but then the other set becomes very large. The question was raised – originally in the context of integers – and the first quantitative result obtained by Erdős and Szemerédi [10], leading to the renowned conjecture:
Conjecture 1. Let \( A \subset \mathbb{R} \). Then
\[
\max(|A + A|, |A \cdot A|) \gtrsim |A|^2.
\]

To avoid trivialities we further assume the \( 0 \notin A \) and \( |A| > 1 \), this will be implicit in all statements we make, as well as that the sets \( A, B, C, \ldots \) are finite.

As usual, we use the notation \(|\cdot|\) for cardinalities of finite sets. The symbols \( \ll, \gg \), suppress absolute constants in inequalities, as do their respective equivalents \( O \) and \( \Omega \). Besides, \( X = \Theta(Y) \) means that \( X = O(Y) \) and \( X = \Omega(Y) \).

In addition, e.g., in the above statement of Conjecture \([1]\) the symbols \( \lesssim, \gtrsim, \sim \) are used to replace, respectively \( O, \Omega, \Theta \) when the inequalities involved are weakened by a power of \( \log |A| \). Thus \( |A| \) is viewed as an asymptotic parameter. The suppressed constants are therefore independent of \( |A| \).

If \( \mathbb{F} \) has positive characteristic \( p \), we only deal with a “small set” case, \( |A| \) being at most some less-than-1 power of \( p \), so \( p \), always denoting the positive characteristic of \( \mathbb{F} \), is regarded as an asymptotic parameter as well.

The sum-product conjecture remains open although current world records in \([17]\) for the reals and \([20], [1]\) in positive characteristic have edged nearer to the statement of the conjecture.

Fundamental to the study of the sum-product phenomenon is a \( L^2 \) quantity expressing the additivity or multiplicativity of a set, known as energy. The additive energy between sets \( A \) and \( B \) is defined as
\[
E^+(A, B) := |\{(a_1, a_2; b_1, b_2) \in A^2 \times B^2 : a_1 + b_1 = a_2 + b_2\}|.
\]
We write \( E^+(A, A) = E^+(A) \); if this quantity is considerably larger than the trivial lower bound \( |A|^2 \) (and closer to the trivial upper bound \( |A|^3 \)), we say \( A \) has an additive structure.

The multiplicative energy \( E^*(A, B), E^*(A) \) is defined similarly. The Cauchy-Schwarz inequality relates the energy to the Erdős-Szemerédi conjecture:
\[
E^+(A)|A + A|, \ E^*(A)|A \cdot A| \gtrsim |A|^4.
\]
Note that by rearranging the equation defining energy, say \( A + A \) in \([1]\) can be replaced by \( A - A \), even though the latter two sets may in principle differ quite a bit.

Geometrically, the multiplicative energy \( E^*(A) \) equals the number of ordered pairs of points of the plane set \( A \times A \), supported on lines through the origin (corresponding to ratios in \( A/A \)). The additive energy \( E^+(A) \) equals the number of ordered pairs of points of \( A \times A \) on parallel lines with the slope plus or minus 1.

To what quantitative extent do additive and multiplicative structure find it hard to coexist in a set? Recently Balog and Wooley \([2]\) raised an interesting question as to whether the correct energy, that is \( L^2 \), formulation of Conjecture \([1]\). If one believes that one of \( |A + A| \) or \( |A \cdot A| \) must be \( \gtrsim |A|^2 \), can both \( E^+(A) \) and \( E^*(A) \) be nonetheless large? An easy example shows, yes: take \( A \) as the union of two disjoint equal in size arithmetic and geometric progressions. Then both energies are \( \Omega(|A|^3) \), that is, up to constants, as big as it gets. Moreover, any subset containing more than, say 51% of \( A \) would have both energies \( \Omega(|A|^3) \). On the other hand, for either
Let $E^+$, or $E^x$, one can find a subset containing every second member of $A$, where the corresponding energy is $\lesssim |A|^2$.

It is possible to intertwine an arithmetic and geometric progression in a smarter way to ensure that any subset of $A$ containing a positive proportion of its members, has both energies considerably in excess of $|A|^2$. Balog and Wooley constructed such an example over the integers. We take a moment to review it briefly, owing to its appeal.

Let $A$ be the union of $n$ disjoint dilates of the integer interval $I = [n^2, \ldots, 2n^2]$ by factors $1, 2, \ldots, 2^{n-1}$. Note that $A \times A$ contains the union of $n$ disjoint square grids $P = (I \times I) \cup (2I \times 2I) \cup \ldots \cup (2^{n-1}I \times 2^{n-1}I)$. Then $E^+(A) \gg |A|^{7/3}$ (sum of additive energies of each grid in $P$) while $E^x(A) \gg |A|^{7/3} \log^4 |A|$, because of (1) and the fact that $|A \cdot A| \sim n^5$. (See [11] proving the explicit value of $s = 0.086\ldots$) If $A' \subset A$ has cardinality $\alpha |A|$, for $0 < \alpha < 1$, it is easy to estimate $E^+(A')$ from below just by looking at intersections $A' \times A'$ with $P$; the minimum estimate is achieved when $A' \times A'$ intersects each square forming $P$ uniformly at $(\alpha n^2)^2$ points. For $E^+(A')$ use (1) and the obvious inclusion $A' \cdot A' \subseteq A \cdot A$. Thus

$$E^+(A'), E^x(A') \gg \alpha^4 n^7 = \alpha^4 \Theta(|A|^{7/3}).$$

Besides, $E^x(A')$ actually exceeds the right-hand side by a power of $\log |A|$. By slight manipulations with the number $n$ of dilates of $I$ versus its size $n^2$, one can easily ensure that the logarithmic factor in $|A|$ is present in the estimate for both energies of $A'$.

The Balog–Wooley example shows that even though multiplicative and additive structure may not conjecturally coexist in any $A$ in the strong sense of Conjecture 1 they cannot be completely divorced in the $L^2$ sense even by taking reasonably small subsets. On the other hand, we do not believe that the standard construction arsenal offers a stronger one than described above. It seems likely that the following claim is true.

**Conjecture 2.** Let $A \subset \mathbb{R}$. There exists $A' \subseteq A$, such that $|A'| \geq |A|/2$, and

$$\min\{E^+(A'), E^x(A')\} \lesssim |A|^{7/3}.$$

Note that trivially we cannot expect to destroy multiplicative (respectively additive) structure by taking a subset, unless the latter is very thin, as is the case if, for example, $A$ is a geometric (respectively arithmetic) progression.

Balog and Wooley formulated their results in terms of the decomposition of $A$ as follows.

**Theorem 1 ([2]).** Let $A \subset \mathbb{R}$ be a set and $\delta = 2/33$. Then there are two disjoint subsets $B$ and $C$ of $A$ such that $A = B \sqcup C$ and

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

**Remark 1.** The sum-product phenomenon is not restricted specifically to reals. Its study in prime residue fields $\mathbb{F}_p$ was initiated by Bourgain, Katz, and Tao [6]. If the field $\mathbb{F}$ has positive characteristic $p > 0$, we consider the case when $A$ is suitably small in terms of $p$. We do not know of any evidence that Conjectures 1, 2 may be false if, say $|A| < p^{1/3}$. To this end [2] contains a positive characteristic version
of Theorem 1 with a smaller value of $\delta = 4/101$, subject to the constraint roughly $|A| < p^{101/161}$.

The two main ingredients of the argument in [2] were the two following geometric incidence theorems and additive combinatorics. The known sum-product results over the real or complex field are somewhat stronger than in fields of positive characteristic largely due to order properties of reals, which so far have been indispensable for proofs of the celebrated Szemerédi-Trotter theorem in the plane. See [30], [32] for the original proof for reals and subsequent extension to the complex field.

**Theorem 2 (Szemerédi-Trotter Theorem).** The number of incidences between a set of $m$ lines and $n$ points in $\mathbb{C}^2$ is $O((mn)^{2/3} + m + n)$.

For arbitrary fields the first author proved a weaker geometric incidence theorem in $\mathbb{F}^3$.

**Theorem 3 ([21]).** The number of incidences between a set of $m$ planes and $n \leq m$ points in $\mathbb{F}^3$ is $O(m(n^{1/2} + k))$, where $k$ is the maximum number of collinear points, under an additional constraint $n \leq p^2$ in positive characteristic.

Thus real or complex numbers will be the special case in the sequel, and since $\mathbb{R}$ is not special for the ensuing discussion versus $\mathbb{C}$, we formulate the corresponding results in terms of the latter field.

It was shown in [1] that Theorem 3 implies a weaker version of the Szemerédi-Trotter theorem for a general $\mathbb{F}$, with the main term $m^{3/4}n^{2/3}$ if the point set is a Cartesian product $A \times B$, with $|B| \leq |A| \leq p^2$ in positive characteristic. This was recently improved by the third author and de Zeeuw and generalised to arbitrary point sets as follows.

**Theorem 4 ([29]).** Consider a set of $m$ lines in $\mathbb{F}^2$.

(i) Let $A \times B \subset \mathbb{F}^2$ be a set of $n$ points, with $n^{1/2} < m < n^{3/2}$ and the constraint $mn^2 < p^4$ in positive characteristic. The number of incidences between the above sets of points and lines is $O(m^{3/4}n^{5/8})$.

(ii) For any set of $n$ points in $\mathbb{F}^2$, with $n^{7/8} < m < n^{8/7}$ and $m^{13}n^{-2} < p^{15}$, the number of incidences with the set of $m$ lines is $O((mn)^{11/15})$.

Incidence theorems have been widely used in arithmetic combinatorics. Elekes [8] realised that Theorem 2 applies to sum-product type problems and proved the following estimate towards Conjecture 1:

$$\max(|A + A|, |A \cdot A|) \gg |A|^{1+\delta}, \quad \delta = 1/4. \quad (2)$$

Roche-Newton and the first two authors [20] applied Theorem 3 in a similar vein and proved, for any field $\mathbb{F}$, that

$$\max(|A + A|, |A \cdot A|) \gg |A|^{1+\delta}, \quad \delta = 1/5. \quad (3)$$

under an additional constraint $|A| \leq p^{5/8}$ in positive characteristic.

There has been a series of improvements of the estimate (2) in the real and complex case, started by Solymosi [27], and currently up to $\gtrsim |A|^{3+\delta} \cdot \sqrt{n}$ in the right-hand
side by Konyagin and the second author [17]. All such improvements of (2) (see, e.g., the references in [17]) used crucially the order properties of the reals (the arguments would usually generalise to \( \mathbb{C} \), see for example [15]) and benefited by repeated applications of the Szemerédi-Trotter theorem involving the sets of sums or products themselves. Without order in (a subfield of) \( \mathbb{F} \), the sum-product estimate (3) is the best one known.

Our main result is the following theorem, which implies, up to factors of \( \log |A| \), the latter two estimates in the context of Conjecture 2. We establish the following:

**Theorem 5.** Let \( A \subset \mathbb{F} \). There exists \( A' \subseteq A \), such that \( |A'| \geq |A|/2 \), and 
\[
\min [E^+(A'), E^\times (A')] \lesssim |A|^{3-\delta},
\]
where \( \delta = 1/4 \) in the special case \( \mathbb{F} = \mathbb{C} \) and \( \delta = 1/5 \) for any \( \mathbb{F} \), with an additional constraint \( |A| \leq p^{5/8} \) in positive characteristic.

Theorem 5 is an immediate consequence of the forthcoming, and stronger, Theorem 7 which is an improvement of Theorem 1. The values of \( \delta \) we establish match those in the estimates (2), (3). Thus, our arguments emphasise the geometric (and reduce the additive) combinatorics content of the proof: passing from the estimates (2), (3) to their weaker \( L^2 \) formulation in Theorem 5 only incurs logarithmic factors in \( |A| \).

Since these estimates are, of course, partial apropos of Conjecture 2 we have not troubled ourselves with calculating the exact powers of \( \log |A| \). On the other hand, we do not expect that, modulo these factors, the estimates in question can be improved within today’s state of the art toolkit. Once again, all the improvements of the Elekes estimate (2) in the real/complex case appear to relate (multiplicative or additive) energy to the size of the counterpart (respectively product or sum) set and do not work in the energy-energy sense, cf. the title of the breakthrough paper [28] by Solymosi.

These improvements, in particular were enabled by the idea of the second author and Schoen to use the third, rather the second moment, or cubic (and higher order) energy of the convolution function arising in the description of sum or product sets. See, e.g., [23]. This opportunity is inherent in the numerical values of the exponents arising in the Szemerédi-Trotter theorem. It does not appear to be granted by the weaker Theorem 3. Nor does it seem to be at hand if one pursues energy-energy estimates. This is why, we believe, Theorem 5 marks a certain milestone, and to improve its exponents, which are \( \delta = 1/4 \) for \( \mathbb{F} = \mathbb{C} \) and \( \delta = 1/5 \) otherwise, one needs a conceptual innovation, whether this is about the reals or a general \( \mathbb{F} \).

On the technical level we do much better than Theorem 1 by avoiding the use of the Balog-Szemerédi-Gowers theorem. The latter, presented as Theorem 14 below, has been a standard arithmetic combinatorial tool for passing from large energy bounds to subsets with small doubling, in particular Balog and Wooley used it to prove Theorem 1. Unfortunately, on the quantitative level applying the Balog-Szemerédi-Gowers theorem is usually quite wasteful. Konyagin and the second author found a way to avoid it in the context of Theorem 1 where they proved \( \delta = 1/5 \) over the reals [17]. In the proof of the key result of this paper, the forthcoming Theorem 7
we follow the main line of the argument in Section 4 of [17], making it somewhat stronger, which yields what we believe is the strongest result, within reach of today’s machinery, that is $\delta = 1/4$ for real and complex numbers.

We develop the argument in the context of a general field $\mathbb{F}$, where we use Theorem 3 while Theorem 2 applies to $\mathbb{F} = \mathbb{C}$ as a special case. This enables us to prove $\delta = 1/5$ for a general $\mathbb{F}$, matching its value in the sum-product estimate (3), while $\delta = 1/4$ for $\mathbb{F} = \mathbb{C}$, matches the Elekes estimate (2).

As far as applications are concerned, we are interested in quantitative arithmetic growth estimates. By arithmetic growth we mean, for an integer $n \geq 2$, having a function $f : \mathbb{F}^n \to \mathbb{F}$, such that for any $A \subset \mathbb{F}$, sufficiently small in terms of $p$ in the positive characteristic case, the cardinality of the range of $f$, restricted to $A^n$, exceeds $|A|$ by orders of magnitude. See [1] and the references contained therein for some quantitative estimates for $n = 2, 3, 4$ over general fields and general discussion.

It appears that our energy method enables one to obtain stronger quantitative growth estimates, for they often result in a relation binding energies of two different types, say $E^\times(A)$ and $E^+(A)$ for some putative set $A$. Our results, see the forthcoming Corollary 8 provide upper bounds for the product of the two energies if one passes to a pair of large subsets. Previously available estimates would bind, say multiplicative energy and the sum set, see e.g., [28]. Passing from $E^+(A)$ to the sum set, aiming basically to invert the first inequality in (1) would invoke a quantitatively costly application of the Balog-Szemerédi-Gowers theorem. Our method enables one to bypass this.

There is a well established connection between arithmetic growth and incidence geometry estimates, in both directions. However exploring this connection from the former towards the latter estimates would invariably invoke the Balog-Szemerédi-Gowers theorem. We limit the references to the well-known works of Bourgain, Katz and Tao [6] and Green and Tao [13]; see Section 6 in both papers. It turns out, however, that the Balog-Szemerédi-Gowers theorem can be avoided. In the context of incidence estimates, namely Theorem 4 (ii), this was achieved in [29]. In the same vein, we challenge an interested reader to embark on reducing – and strengthening – the fairly lengthy proof of Proposition 6.6 in [13] to a much shorter energy argument, avoiding the Balog-Szemerédi-Gowers theorem in the vein of the forthcoming Theorem 9.

We presently limit the number of applications considered in detail to one, concerning the prime residue field $\mathbb{F}_p$. Given $f : \mathbb{F}_p^n \to \mathbb{F}_p$, what is the lower bound on $|A|$, such that for any $A \subset \mathbb{F}_p$, the range of $f$, restricted to $A^n$, takes up a positive proportion of the field $\mathbb{F}_p$? For many such $f$ one can relatively easily prove the threshold $|A| = \Omega(p^{2/3})$, via character sums or often just linear algebra methods that work well for relatively large sets with respect to $p$. See e.g [7]. However, these techniques usually fail to work for smaller $A$. To this effect, the challenge is to reduce the threshold $|A| = \Omega(p^{2/3})$ for some $f$.

Petridis [19] proved recently that if $|A| \geq p^{5/8}$, then the cardinalities of the sets $(A + A) \cdot (A + A)$, $(A + A)/(A + A)$ are both $\Omega(p)$, having incorporated the so-called “generic projections” argument from [6] and Theorem 3 into a rather involved
argument. Generic projections is an easy pigeonholing argument showing that the sets \((A - A)/(A - A)\), as well as \(\{\frac{a-c}{a-d} : a, b, c, d \in A, a \neq d\}\) are both equal to \(\mathbb{F}_p\) as long as \(|A| > p^{1/2}\).

As a matter of fact, Petridis establishes a stronger \(L^2\) claim that the number of solutions of the equation
\[(a + b)(c + d) = (a' + b')(c' + d') : a, \ldots, d' \in A\]
is bounded as \(O(|A|^8/p)\), that is up to a constant the expected number, as long as \(|A| > p^{5/8}\). Such a bound appears to be out of reach by methods of [6] even regarding the set \((A - A)/(A - A)\) if one rearranges the latter equation as fractions and replaces the plus signs by minuses.

In this paper we establish the following.

**Theorem 6.** Let \(A \subseteq \mathbb{F}_p\), with \(|A| \gg p^{25/42}\log^K |A|\), for some absolute constant \(K\). There are disjoint \(B, C \subset A\), each of cardinality \(\geq |A|/3\), such that number of solutions to the equation
\[(4) \quad \frac{ab - c}{a - d} = \frac{a'b' - c'}{a' - d'} : a, b, a', b', c, d, c', d' \in C\]
is \(O(|A|^8/p)\), and therefore \(\left|\left\{\frac{ab - c}{a - d} : a, b, c, d \in A\right\}\right| = \Omega(p)\).

The reader can verify that in the latter theorem all the minus signs can be replaced by plus signs as well.

### 2.1. Further results.

Here we present a somewhat stronger formulation of Theorem 5, its analogue for multiplicative energies of additive shifts and the energy version of the Elekes-Ruzsa few sums, many products inequality. The latter is available only in the real/complex setting; over the reals it yields a minor improvement of the best known sum-product exponent, after being plugged into the argument recently developed by Konyagin and the second author. We also provide an auxiliary subsection which contains a suitably tailored version of the Balog-Szemerédi-Gowers theorem – which may be interesting in its own right – and some indication of what our results would look like if the Balog-Szemerédi-Gowers theorem had to be used.

#### 2.1.1. Sum-product decomposition and energy inequalities.

**Theorem 7** (Balog-Wooley decomposition). Let \(A \subset \mathbb{F}\). There exist two disjoint subsets \(B\) and \(C\) of \(A\), such that \(A = B \sqcup C\), and
\[
\max\{E^+(B), E^+(C)\} \lesssim |A|^{3 - \delta},
\]
where \(\delta = 1/4\) in the special case \(\mathbb{F} = \mathbb{C}\) and \(\delta = 1/5\) for any \(\mathbb{F}\), with an additional constraint \(|A| \leq p^{5/8}\) in positive characteristic.

Theorem 7 clearly implies Theorem 5 one of \(B, C\) has size \(\geq |A|/2\).

As we have mentioned, one cannot expect both \(B\) and \(C\) in Theorem 7 to constitute a positive proportion of \(A\). But this can be achieved by weakening the claim as follows, to be used in the proof of Theorem 6.
Corollary 8. Let $A \subset \mathbb{F}$, with an additional constraint $|A| \leq p^{3/5}$ in positive characteristic. There exist two disjoint subsets $B$ and $C$ of $A$, each of cardinality $\geq |A|/3$, such that

$$E^+(B) \cdot E^x(C)^{3/2} \lesssim |A|^7.$$  

In the latter estimate the additive and multiplicative energy can be swapped (for some other $B, C$). Besides, there exist two disjoint subsets $B$ and $C$ of $A$, each of cardinality $\Omega(|A|)$, such that

$$E^+(B) \cdot E^x(C) \lesssim |A|^{28/5}.$$  

Furthermore, if $\mathbb{F} = \mathbb{C}$, the estimate (5) improves to

$$E^+(B) \cdot E^x(C) \lesssim |A|^{11/2}.$$  

We will spell out the proof of Theorem 7, the key quantitative result, in all detail. This proof, furthermore, allows for a number of straightforward variations, which result from the fact established in the quoted literature. Some of these variations are left without detailed proofs, for they would repeat the main arguments more or less line by line.

2.1.2. Multiplicative energy of translates. In [25] the second author considers a slightly more general context than usual sum–products setting. The proof of Theorem 7 combined with the arguments of [17], enables one to establish a variant of Theorem 7 as follows.

Theorem 9. Let $A \subset \mathbb{C}$ be a set, $\alpha \neq 0$, and $\delta = 1/4$. Then there are two disjoint subsets $B$ and $C$ of $A$ such that $A = B \cup C$ and

$$\max\{E^x(B), E^x(\alpha + C)\} \lesssim |A|^{3-\delta}.$$  

Further, there are disjoint subsets $B'$ and $C'$ of $A$ such that $A = B' \cup C'$ and

$$\max\{E^+(B'), E^+(1/C')\} \lesssim |A|^{3-\delta}.$$  

We will further present a proof of the following consequence of Theorem 9, which improves a result from [26].

Corollary 10. Let $A \subset \mathbb{C}$ be a set, and let

$$R[A] := \left\{ \frac{a_1 - a}{a_2 - a} : a, a_1, a_2 \in A, a_2 \neq a \right\}.$$  

Then there are two sets $R', R'' \subset R[A]$, $|R'|, |R''| \geq |R[A]|/2$ such that $E^x(R') \lesssim |R'|^{3-1/4}$ and $E^+(R'') \lesssim |R''|^{3-1/4}$.

Note that the set $R[A]$ is the set of finite pinned cross-ratios, generated by the projective set $A \cup \{\infty\}$, defined by quadruples $(a, a_1, a_2, \infty)$. 
Naturally, an analogue of Theorem 9 over a general field $F$, following from the proof of Theorem 7 also exists. It is established by combining the arguments of the proof of Theorem 7 and the proof of Proposition 2 in [17].

**Theorem 11.** Let $A \subset F$. If $F$ has positive characteristic $p$, suppose $|A| \leq p^{5/8}$. Let $\alpha \in F^*$ and $\delta = 1/5$. Then there are two disjoint subsets $B$ and $C$ of $A$ such that $A = B \sqcup C$ and

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

We cannot obtain an equally strong analogue for the second statement of Theorem 9 about the set of the reciprocals. Extending the bound (9) to general fields would require incidence results for hyperbolae rather than affine objects. However, a weaker result can most likely be derived on the basis of Proposition 14 in [1].

In addition, Corollary 8 also applies if one replaces the two energies appearing therein by multiplicative energies of two distinct translates of $A$.

2.1.3. Few Sums, Many Products. Our approach also allows for the energy generalisation of the well-known result of Elekes and Ruzsa, from the paper [9], whose title we have used for this subsection. Namely, for $A \subset \mathbb{R}$ (as well as of $\mathbb{C}$) one has

$$|A + A|^3|AA| \gtrsim |A|^6$$

In fact, we strengthen the above result to an energy-energy inequality, which is “morally” equivalent to $|A + A|^3|AA| \gtrsim |A|^5$. We present the result as an energy inequality and remark that for general fields we do not have an analogue that would be stronger than (5) in Corollary 8.

**Theorem 12.** Let $A \subset \mathbb{C}$. There exist two disjoint subsets $B$ and $C$ of $A$, each of cardinality $\geq |A|/3$, such that

$$(10) \quad E^\times(B) \cdot E^+(C)^3 \lesssim |A|^{11}.$$ 

However, since the exponents 1, 3 in the above estimate are quite far from one another, estimate (10) beats the non-optimal estimate (7) only if the additive anergy is sufficiently large. Besides, the two energies cannot be swapped in Theorem 12.

2.1.4. The sum-product estimate over $\mathbb{R}$. Theorem 12 yields a minor improvement of the stat-of-the-art sum-product exponent over the reals. Konyagin and the second author [16, 17] set a new world record towards Conjecture 1, having shown that for a finite set $A$ of reals,

$$\max(||A + A||, |A \cdot A|) \gtrsim |A|^{\frac{1}{4} + \frac{1}{18913}}.$$ 

\[\text{1} \] The proof merely requires replacing the equation (17) in the proof of the forthcoming Proposition 16 by the equation corresponding to the energy $E^\times(\alpha + A_1)$, rather than $E^+(A_1)$, where $A_1 \subset A$ is constructed throughout the proof of Proposition 16. One proceeds by applying Theorem 9 to the latter equation in essentially the same way it is done in the proof of Proposition 16; the actual application of the theorem can be copied from the proof of Proposition 2 of [1].
This improved the previous best-known exponent \( \frac{4}{3} \) obtained some ten years earlier as a result of a graceful and renowned construction by Solymosi \[28\], which only relies on the order properties of reals and does not use the Szemerédi-Trotter theorem. Within the arguments in \[16\], \[17\], the margin by which the value \( \frac{4}{3} \) can be beaten depends on the best known estimates apropos of two issues, which can be described as “few products, many sums” and “few sums, many products”. The current approach to both issues that furnishes sufficiently strong estimates is largely based on the Szemerédi-Trotter theorem. Dealing with the “few sums, many products” side of the coin has been much more successful; this was first done by Elekes and Ruzsa \[9\]. Its counterpart proves to be much harder; it is referred by some authors as the \textit{weak Erdős-Szemerédi conjecture}, with the best known estimate stated as \[17\, \text{Theorem 12}\], originating in \[24\].

Konyagin and the second author proved an energy version of the estimate of Elekes and Ruzsa \[16\, \text{Theorem 9}\]; it is slightly weaker than estimate \[10\] above herein. The following improvement of the sum-product inequality \[11\] comes after a calculation if one replaces the estimate of \[16\, \text{Theorem 9}\] with a variant of estimate \[10\]. This improves the estimates of \[17\, \text{Lemma 18}\] and if one chases through the ensuing \[17\, \text{Proof of Theorem 3}\], the result becomes as follows.

\textbf{Corollary 13.} For a finite set \( A \subseteq \mathbb{R} \), one has
\[
\max(|A + A|, |A \cdot A|) \gtrsim |A|^\frac{4}{3} + \frac{1}{1509}.
\]

\section{Balog-Szemerédi-Gowers Theorem.}

We present some auxiliary results in this short section as a weaker, but arguably less technical alternative to the forthcoming key Propositions \[16\, \text{17}\]. In contrast, this section is about the Balog–Szemerédi–Gowers theorem \[12\], which our main proofs avoid. We take advantage of the opportunity to present a small but potentially useful modification of one result from Schoen’s paper \[22\]. For modern forms of the Balog-Szemerédi-Gowers theorem see, e.g., \[5\] and \[22\].

It is easy to see that the following statement implies the original Balog–Szemerédi–Gowers theorem.

\textbf{Theorem 14.} Let \((G, +)\) be an abelian group. Let \( A \subseteq G \) be a set, \( K \geq 1 \) be a real number, and \( k \geq 2 \) be an integer. Suppose that \( E^+(A) \geq |A|^3/K \). Then there are sets \( A_1 \subseteq A, P \subseteq A - A \) such that \( |A_1| \geq |A|/(8kK), |P| \leq 8kK|A| \) and for any \( a_1, \ldots, a_k \in A_1 \) one has
\[
|A \cap (P + a_1) \cap \cdots \cap (P + a_k)| \geq \frac{|A|}{4K}.
\]

Theorem \[14\] allows, e.g., for the following analogue of the forthcoming key Proposition \[17\], which basically stand for the Balog-Wooley decomposition. The estimates are weaker but proofs are simpler.

\textbf{Proposition 15.} Let \( A \subseteq \mathbb{C} \) be a set. Then there is \( A_1 \subseteq A \) such that \( |A_1| \gtrsim E^\times(A)|A|^{-2} \) and
\[
|A_1| \gtrsim |A|^3 \quad \text{and} \quad (E^+(A_1))^2(E^\times(A))^9 \lesssim |A|^3/29.
\]
The special case $F = \mathbb{C}$ in the above formulation indicates the use of the Szemerédi-Trotter theorem in the proof below. We challenge an interested reader to formulate a general field analogue, replacing the use of Theorem 2 by Theorem 4.

3. PROOF OF THEOREM 7

We start out with two intermediate results towards the estimate of Theorem 7; one will later result in $\delta = 1/5$ for a general $F$ and the other in $\delta = 1/4$ for $F = \mathbb{C}$ in Theorem 7.

Proposition 16. Let $A \subset F$, with $|A|^6 \lesssim p^2 E^x(A)$ in positive characteristic. Then there is a set $A_1 \subset A$ such that $|A_1| \gtrsim \sqrt{E^x(A)/|A|}$ and

$$E^+(A_1) \lesssim |A_1|^{11/2}|A|^{3/2}(E^x(A))^{-3/2}. \tag{14}$$

The energies $E^x, E^+$ in the above statement can be swapped (for some other $A_1$).

Proof. Using the pigeonhole principle, we choose a dyadic group $P$ of ratios from $A/A$, with approximately some $t$ realisations, which supports at least a fraction of $\frac{1}{\log_2|A|}$ of $E^x(A)$. More precisely, there is a set $P \subset A/A$ and an integer $t$, such that $|A|^t/(2|A/A|) \leq t \leq |A|$. Let $\pi_x : A \to A'$ be the projection of points of $A$ to the $x$-axis: $\pi_x(s_x, s_y) = s_x$. The projection $\pi_y$ is similarly defined as the projection to the set of ordinates.

Consider the set $A_x$ of abscissae of $S$, that is $A_x = \pi_x(S)$. By another dyadic pigeonhole argument, we find a set $A' \subset A_x$ of popular abscissae for $S$. There exists $A' \subset A_x$, and a number $q'$ such that for every $x' \in A'$, the vertical line through $x'$ supports approximately $q'$ points of $S$ (more precisely $q' < |S \cap \{x = x'\}| \leq 2q'$), and $|A'q'| \sim |S|$. Observe that $q' \leq \min(|A|, |P|)$, but in the sequel we need an analogue of the slightly stronger inequality $q' \lesssim |A'|$, which is not necessarily true.

So if $q' \leq |A'|$ then we set $A_1 = A'$ and $q = q'$. Otherwise we do another dyadic pigeonholing, now by ordinates. I.e., we consider the plane set $S' = S \cap \pi_x^{-1}(A')$ and find a number $q''$ and a set $A'' \subset \pi_y(S')$ such that $q'' < |S' \cap \{y = y''\}| \leq 2q''$ for all $y'' \in A''$. In other words, $A''$ is the set of popular ordinates of the set $S'$ (which in turn is almost as big as $S$): the horizontal line through each $y \in A''$ contains about $q''$ points of $S'$. We have

$$q'|A'| \sim q''|A''|$$

and since clearly $q'' \leq |A'|$, plus since we assume $q' > |A'|$, we must have $|A''| \gtrsim q' > |A'| \gtrsim q''$. We conclude that $q'' < q' \lesssim |A''|$ and set $A_1 = A''$ and $q = q''$.

Hence now $|A_1| \gtrsim q$, and so we have

$$|A_1|^2 \gtrsim q|A_1| \sim |S| \sim |P|t^2/t \sim \frac{E^x(A)}{t} \gtrsim \frac{E^x(A)}{|A|}. \tag{15}$$
Besides, since $|P|t \leq |S| \lesssim |A_1|^2$, and $t^2 \sim E^\times(A)/|P|$ we conclude that
\begin{equation}
|P| \lesssim |A_1|^4/E^\times(A).
\end{equation}

Without loss of generality let us regard $A_1 = A'$, that is the set of popular abscissae, rather than ordinates. We then have by construction of $A'$ a set, each member of which can be represented at least $q$ times as a ratio from $A/P$:
\begin{equation}
E^+(A_1) = |\{(a,a',b,b') \in A_1^2 : a + b = a' + b'\}|
\end{equation}
\begin{equation}
\leq q^{-2}|\{(a,a',p_*p',\alpha,\alpha') \in A_1^2 \times P^2 \times A^2 : a + \alpha/p_* = a' + \alpha'/p'\}|
\end{equation}

Note that by symmetry of $A \times A$, $P = P^{-1}$, so we can (but do not have to – this is only a gesture towards the fact that there is no difference as to whether $A_1$ has been taken as $A'$ or $A''$) replace division by $p$ by multiplication.

Consider then the family of $m = |A_1||P||A|$ planes, with equations $a + p_*x = y + \alpha'z$ : $(a,p_*,\alpha') \in A \times P \times A$ and the same number of points $(x,y,z) \in P \times A_1 \times A$. Applying Theorem 3 we claim that, in terms of the contribution of the main term $m^{3/2}$ in the estimate of the Theorem
\begin{equation}
E^+(A_1) \ll (|A||P||A_1|)^{3/2}q^{-2},
\end{equation}
to be fully justified shortly.

Indeed, the maximum number of collinear points $k$ in the estimate of Theorem 3 is bounded by $\max(|A_1|,|P|)$. If the maximum equals $|P|$ then to drop the $km$ term in the estimate of Theorem 3 it therefore suffices to show that $|P| \lesssim |A||A_1|$. This is true, since we have established that $|P| \lesssim |A_1|^2$. Now if $\max(|A_1|,|P|) = |A|$ then we need to check $|A| \lesssim |A_1||P|$. But $|P| \geq E^\times(A)/|A_1|^2$ and hence everything follows from a trivial bound $E^\times(A) \geq |A|^2 \geq |A_1||A|$.

In positive characteristic Theorem 3 is applicable when $|A_1||P||A| \leq p^2$. By (16) and the trivial bound $|A_1| \leq |A|$, this will be true given that $|A|^6 \lesssim p^2E^\times(A)$. To strengthen the latter constraint to $|A|^6 \leq p^2E^\times(A)$, as claimed, we proceed as follows.

Suppose, $|A|^6 \leq p^2E^\times(A)$. Partition the set of points $P \times A_1 \times A$ in $\lesssim 1$ pieces $\{P_i\}$ (say, by partitioning $A$), whose size differs by at most an absolute constant factor, and such that each $|P_i| \leq p^2$. The number of solutions of the equation in the second line of (17) is the sum, over $1 \leq i \lesssim 1$, of the number of incidences between the above $m$ planes and the point set $P_i$. By Theorem 3 it is $O(m^{3/2})$, for each $i$.

Thus the summation over $i \lesssim 1$ results only in the change of the power of $|A|$ hidden in the incidence estimate (15), that is if $|A|^6 \leq p^2E^\times(A)$ the estimate (18) is true, with a different factor of $\log |A|$ hidden in the $\lesssim$ symbol.

We pass from formula (18) to (14) by setting $q \sim |P|t/|A_1|$, $E^\times(A) \sim |P|^2$ and using (16) to bound the remaining $\sqrt{|P|}$ in the numerator.

We have established the formula (14) as it is. The fact that energies can be swapped follow by taking the above set $P$ as a subset of $A - A$, rather than of $A/A$, and repeat the argument. The only modification is that the equivalent of (17) will now deal with $E^\times(A_1)$, followed by the equivalent of (18), as worked out explicitly in the proof of Proposition 1 in [1].
This completes the proof of Proposition 16.

In the special case of the real or complex field we have a slightly stronger result via the Szemerédi-Trotter theorem.

**Proposition 17.** Let \( A \subset \mathbb{C} \) be a set. Then there is \( A_1 \subseteq A \) such that \( |A_1|^2 \gtrsim E^\times(A)|A|^{-1} \) and

\[
E^+(A_1)E^\times(A) \lesssim |A_1|^{9/2}|A|.
\]

The energies \( E^\times, E^+ \) in the above statement can be swapped (for some other \( A_1 \)).

**Proof.** One repeats the pigeonholing arguments in the proof of Proposition 16 with the same notations \( t, P, q, A_1 \) up to and inclusive of the estimate (16). Without loss of generality we assume that \( A_1 \) is the set of popular abscissae \( A' \) in the construction of Proposition 16.

Using the notation of [16], we observe that

\[
A_1 \subset \text{Sym}_q(A, P) := \{ x : |A \cap xP| \geq q \},
\]

which means that, by construction, each member of \( A_1 \) can be represented at least \( q \) times as a ratio from \( A/P \) (or a product \( AP \), since \( P = P^{-1} \)).

Using Lemma 13 and Corollary 11 of [17] we conclude that

\[
E^+(A_1) \ll d_*(A_1/2)|A_1|^{5/2},
\]

where the parameter (see [17])

\[
d_*(A_1) \leq \frac{|A|^2|P|^2}{q^3|A_1|}.
\]

Using the relations \( |A_1|q \sim |P|t \lesssim |A_1|^2 \) from the proof of Proposition 16 we obtain

\[
d_*(A_1) \sim \frac{|A|^2|A_1|^2}{|P|t^3} \sim \frac{|A|^2|A_1|^2|P|t}{E^\times(A)^2} \sim \frac{|A|^2|A_1|^4}{E^\times(A)^3}.
\]

Substituting the latter estimate into (20) completes the proof of Proposition 17. The fact that the energies \( E^\times, E^+ \) can be swapped follows taking \( P \subseteq A - A \) instead of \( A/A \) and repeating the argument. See also Theorem 20 in [17].

**Remark 2.** The same proof can be easily modified to an application of Theorem 4 here instead of Theorem 3. The latter theorem would also enable one to obtain decomposition estimates involving higher energies, along the lines of those obtained by the second author in [26] over the reals.

We note, however, that the proofs of Propositions 16, 17 use the symmetry between the \( x \) and \( y \)-axes and are not applicable to the quantities \( D^+, D^\times \), studied by the second author in [26].

---

2For a reader not willing to consult [17] we sketch the argument that goes back to the paper of Elekes [8] and is similar to the one in the conclusion of the proof of Proposition 16. Instead of Theorem 3 one uses the Szemerédi-Trotter theorem to estimate the cardinality of the set \( S_\tau \) of sums \( s = a + b \) in \( A_1 + A_1 \) with approximately \( 1 \leq \tau \lesssim |A_1| \) realisations. One can rewrite \( s = a + \alpha p \), with \( \alpha \in A, p \in P^{-1} = P \), and therefore there are at least \( \tau |A_1| \) incidences between the point set \( A \times S_\tau \) and a set of \( |P||A_1| \) lines. Theorem 3 then gives the upper bound on \( |S_\tau| \); recycling this into an energy estimate is a standard exercise.
To conclude the proof of Theorem 7 the above intermediate results are iterated via a simple lemma: see, e.g., [31].

**Lemma 18.** Let $A_1, \ldots, A_n$ be subsets of an abelian group. Then

$$
\left( E^+(\bigcup_{i=1}^n A_i) \right)^{1/4} \leq \sum_{i=1}^n (E^+(A_i))^{1/4}.
$$

Observe that Propositions 16, 17 imply a weaker version of Theorem 7, where one replaces $\max(B, C)$ with $\min(B, C)$.

### 3.0.1. Conclusion of the proof of Theorem 7 and proofs of Corollary 8

**Conclusion of the proof of Theorem 7.** Suppose $E^+(A) \lesssim |A|^{3-\delta}$ or there is nothing to prove: we can always take a small $B$ such that $|B|^3 < |A|^{3-\delta}$ and $C = A \setminus B$. Heuristically, we use Proposition 16 for a general $F$ and Proposition 17 in the special case $F = \mathbb{R}$ or $\mathbb{C}$ to pull out from $A$, one by one, subsets $A_1$ with a small additive energy and stop once the energy of the remainder $C$ of $A$ will become smaller than $|A|^{3-\delta}$. This is bound to happen if $C$ becomes sufficiently small relative to $|A|$. The above lemmas are going to guarantee that $E^+(B = A \setminus C) \lesssim |A|^{3-\delta}$.

Formally, let $M \geq 1$ be a parameter which we choose later, assume that $E^+(A) \leq |A|^3/M$ and $|A|^3 \leq p^2/M$ in positive characteristic.

We construct a decreasing sequence of sets $C_1 = A \supseteq C_2 \supseteq \cdots \supseteq C_k$ and an increasing sequence of sets $B_0 = \emptyset \subseteq B_1 \subseteq \cdots \subseteq B_{k-1} \subseteq A$ such that for any $j = 1, 2, \ldots, k$ the sets $C_j$ and $B_{j-1}$ are disjoint and moreover $A = C_j \cup B_{j-1}$. If at some step $j$ we have $E^+(C_j) \leq |A|^3/M$, we stop and set $C = C_j$, $B = B_{j-1}$, and $k = j-1$. Else, we have $E^+(C_j) > |A|^3/M$. We apply Proposition 16 to the set $C_j$, finding the subset $D_j$ of $C_j$ such that

$$
|D_j|^2 \gtrsim \frac{E^+(C_j)}{|C_j|} > \frac{|A|^3}{M|C_j|} \geq \frac{|A|^2}{M}.
$$

and

$$
E^+(D_j) \lesssim \frac{|D_j|^{11/2} |C_j|^{3/2}}{(E^+(C_j))^{3/2}} \leq \frac{M^{3/2} |D_j|^{11/2} |C_j|^{3/2}}{|A|^{9/2}} < |D_j|^{11/2} M^{3/2} |A|^{-3}.
$$

After that we put $C_{j+1} = C_j \setminus D_j$, $B_j = B_{j-1} \cup D_j$ and repeat the procedure. In view of the uniform lower bound (21) on $|D_j|$, the process will terminate, as $|C_j|$ decreases, after say $k$ iterations, when $E(C = C_{k+1}) \leq |A|^3/M$. We set $B = B_k = \bigcup_{j=1}^k D_j$ and $C = C_{k+1}$, so $A = B \cup C$.

Trivially $|B| = \sum_{j=1}^k |D_j| \leq |A|$. 


Then, using Lemma 18 and the bound (14) of Proposition 16 we get

\[ E^+(B) \lesssim M^{3/2} |A|^{-3} \left( \sum_{j=1}^{k} |D_j|^{11/8} \right)^4 \]
\[ \leq M^{3/2} |A|^{-3} \max_j \{ |D_j| \}^{3/2} \left( \sum_{j=1}^{k} |D_j| \right)^4 \]
\[ \leq M^{3/2} |A|^{5/2}. \]

Optimising over \( M \), with \( E^+(C) \leq |A|^{3} / M \), that is choosing \( M = |A|^{1/5} \), we obtain the result for a general \( F \). In particular, the constraint in terms of \( p \) in positive characteristic boils down to \( |A|^6 < |A|^{3-1/5} p^2 \), so \( |A| \leq p^{5/8} \).

In the special case of \( F = \mathbb{C} \) the analogue of the estimates (22) and (23) comes from using (19), rather than (14). Namely, we have

\[ E^+(D_j) \lesssim \frac{|D_j|^{9/2}|C_j|}{E^+(C_j)} \leq \frac{M|D_j|^{9/2}}{|A|^2} \]

and

\[ E^+(B) \lesssim M|A|^{-2} \left( \sum_{j=1}^{k} |D_j|^{9/8} \right)^4 \leq M|A|^{5/2}. \]

Optimising with \( E^+(C) \leq |A|^{3} / M \), yields \( M = |A|^{1/4} \). This proves Theorem 7. \( \square \)

Proof of Corollary 8. Observe that if \( A \) has a subset \( C \) with \( |C| \geq 2|A|/3 \) and \( E^+(C) \leq |C|^{8/3} \), there is nothing to prove: just take \( B \) as half of \( C \), with the trivial bound \( E^+(B) \leq |A|^3 \) and rename \( C \) as the other half.

Otherwise we repeat the argument in the preceding proof, finishing it at the first instance when either \( E^+(C) = C_{k+1} < |A|^{8/3} \) or \( |B = B_k| > |A|/3 \). Without loss of generality we can assume that in addition to the estimates (22) and (23) we have, say \( |D_j| < |A|/100 \) for every \( j \) (by partitioning \( D_j \) if necessary). Since the sequence of sets \( \{ C_j \} \) is decreasing, we have \( E^+(C) \leq E^+(C_j) \), \( \forall j \leq k+1 \). Hence, in view of (14), the calculation (24) becomes

\[ E^+(B)E^+(C)^{3/2} \lesssim |A|^{3/2} \left( \sum_{j=1}^{k} |D_j|^{11/8} \right)^4 \leq |A|^7, \]

thus proving (5).

Note that Proposition 16 does indeed apply on each step in positive characteristic, for the condition \( |A|^6 \leq p^2 E^+(C) \) is satisfied, since we have assumed \( E^+(C) \geq |A|^{8/3} \) and \( |A| \leq p^{5/8} \).

To derive (6) of the Corollary from (5) we observe that according to the above proofs one can swap the two energies in (5). We do this for the set \( B \). Namely \( B \) gets partitioned into \( B' \) and \( C' \), each of size at least \( |B|/3 \), such that

\[ E^+(B')^{3/2} E^+(C') \lesssim |A|^7. \]
Multiplying the latter two estimates we obtain
\[(E \times (B) E^+(B'))^{3/2} \cdot (E^+(C) E^+(C')) \lesssim |A|^{14}.\]

If \(E \times (B) E^+(B') \leq E^+(C) E^+(C')\), we get
\[(E \times (B) E^+(B'))^{5/2} \lesssim |A|^{14},\]
(and one can replace \(B\) by \(C'\), disjoint from \(B'\)) otherwise we get the same inequality involving the disjoint \(C\) and \(C'\).

Renaming the two subsets in question as \(B\) and \(C\) finishes the proof, the price we've paid is just that \(B\) and \(C\) no longer partition \(A\). \(\square\)

4. Proof of Theorem 12 and Corollary 13

We give a detailed sketch of the proof of Theorem 12, which largely repeats our previous arguments, the key benefit being derived from using an estimate from [18].

Proof. Sketch of proof

We invoke the additive version of the construction in the proof of Proposition 16, with the same notations, to derive a version of the proposition, given by the forthcoming estimate (24).

\(P\) is now a dyadic group of popular sums, with approximately \(t\) realisations each, that supports \(|P|^t \gtrsim E^+(A)\) of additive energy. \(S\) is the corresponding subset of \(A \times A\). \(A_1\) is the set of popular abscissae (ordinates) for \(S\), with approximately \(q\) realisations, and \(q \lesssim |A_1|\).

Moreover, \(|S|t \lesssim |A_1|^2\) and \(|A_1| \gtrsim \sqrt{E^+(A)/|A|}\).

Assuming that \(A\) does not contain zero, consider the multiplicative energy equation
\[
\frac{a}{b} = \frac{a'}{b'} : a, b, a', b' \in A_1.
\]

For the left-hand side there are approximately \(q\) choices to add some \(c \in A\) in the numerator and some \(d \in A\) in the denominator to replace it with
\[
\frac{(a + c) - c}{(b + d) - d} = \frac{s - c}{r - d},
\]
where \(s, r \in P\). Thus \(E^+(A_1)\) is bounded by a constant, times \(q^{-4}\), times the number of solutions of
\[
\frac{s - c}{r - d} = \frac{s' - c'}{r' - d'} \neq 0, \infty : (s, r, s', r') \in P^4, (c, d, c', d') \in A^4.
\]

The latter equation has been studied, in particular in the paper of Murphy, Roche-Newton, and the second author [18] (see Lemma 2.5 therein) which proves the upper bond \(\lesssim |P|^3|A|^3\) for the number of solutions.

Hence, once \(|A_1|^2 \gtrsim q|A_1| \gtrsim |P|t\) we have
\[(24) \quad E^+(A_1) \lesssim q^{-4}|P|^3|A|^3 \lesssim \frac{|P|^3|A|^3}{|P|^4t^4/|A_1|^2} = |A_1|^4|A|^3 \frac{|P|^2t^2}{|P|^3t^6} \lesssim \frac{|A_1|^8|A|^3}{E^+(A)}.\]
A straightforward adaptation of the iterative argument in the first two passages of the proof of Corollary 8 to the latter estimate completes the proof. \[\Box\]

4.1. Proof of Corollary 13. Observe that inequality (24) implies, by Cauchy-Schwarz, that

\[|A_1 \cdot A_1|, |A_1/A_1| \gtrsim \frac{E^+(A)^3}{|A_1|^4|A|^3} \gtrsim \frac{E^+(A)^3}{|A|^7},\]

hence the same lower bound for the supersets \(|A \cdot A|, |A/A|\). In [16, Theorem 9] a weaker estimate was established:

\[|A \cdot A|, |A/A| \gtrsim \frac{E^+(A)^4}{|A|^10},\]

The latter estimate was used to obtain [16, Lemma 12, estimates (34), (36)], restated as [17, Lemma 18, estimates (22), (24)]. If one uses (25) instead, this improves the term \(L^{-16}\) in these estimates to \(L^{-12}\). Recalculating [17, Proof of Theorem 3 from (26) on] yields the new sum-product exponent \(\frac{4}{3} + \frac{1509}{1999}\) as claimed. \[\Box\]

5. Proof of Corollary 10

Proof. Put \(R = R[A], R^* = R \setminus \{0\}\), and \(\delta = 1/4\). Using Theorem 9, we find \(B, C \subseteq R\) such that \(R = B \cup C\) and

\[\max\{E^x(B), E^x(C - 1)\} \lesssim |R|^{3-\delta}.\]

If \(|B| \geq |R|/2\) then we are done. Suppose not. Then \(|C| \geq |R|/2\) and in view of formula \(R = 1 - R\), see [25], we obtain that \(C' := 1 - C \subseteq R\), \(|C'| = |C| \geq |R|/2\) and

\[E^x(C') = E^x(1 - C) = E^x(C - 1) \lesssim |R|^{3-\delta}.\]

So, putting \(R'\) equals \(B\) or \(C'\), we obtain the result. To find the set \(R''\) note that \((R^*)^{-1} = R^*\) and use the second part of Theorem 9. \[\Box\]

The same proof allows us to find a subset \(A_s'\) of the set \(A_s \cup (-A_s)\), \(A_s = A \cap (A+s)\), \(s \in A - A, A \subseteq C\) of cardinality \(|A_s|/2\) such that \(E^x(A_s') \lesssim |A_s'|^{3-1/4}\). This question is a dual of one which appeared in [16], [17]. The same result holds for some multiplicative analogue of the sets \(A_s\), namely, \(A_s^* = A \cap (s/A), s \in AA\).

6. Proof of Theorem 6

We now turn to the proof of Theorem 6. We shall apply Corollary 8 to the set \(A\): it applies when \(|A| \leq p^{3/5}\), which we may assume, passing to a subset if \(A\) is too big.

So, if \(|A| \leq p^{3/5}\), Corollary 8 gives us two positive proportion disjoint subsets \(B, C\) of \(A\), whose energies satisfy the estimate (5) and whereon we consider equation (4).

Let us denote

\[Q = \left\{ \left\{ \frac{ab - c}{a - d} : a, b, c, d \in A, a \neq d \right\} \right\}.\]
By Cauchy-Schwarz

$$\Theta(|A|^8) = |B|^4|C|^4 \leq Q \left( \sum_{x \in \mathbb{F}_p} \left| \left\{ x = \frac{ab - c}{a - d} : a, b \in B; c, d \in C \right\} \right| \right)^2. \tag{26}$$

Let us isolate the case $x = 0$. This means $ab = c$ and $a'b' = c'$, so the trivial bound for this is $|A|^6$.

We can then denote

$$E = \sum_{x \in \mathbb{F}_p^{\neq 0}} \left| \left\{ x = \frac{ab - c}{a - d} : a, b \in B; c, d \in C \right\} \right|^2$$

and assuming $|A| > p^{1/2}$ rewrite (26) as

$$|A|^8 \ll Q E, \tag{27}$$

for trivially $Q \leq p$. We further aim to find the upper bound on $E$.

Rearranging and applying Cauchy-Schwarz once more yields

$$E = \sum_{x \neq 0} |\{ a(b - x) = c - dx \}|^2 \leq \sum_{x \neq 0} E^x(B, x + B) E^+(C, xC). \tag{28}$$

We evaluate these energy terms using an argument of [19], modifying it to suit our needs. Although [19] considers the term containing $E^+(C, xC)$ only, the analysis applies almost verbatim to the quantity $E^x(B, x + B)$ as well.

In the following lemmata, $A$ denotes a dummy set, to be replaced, respectively, by $C$ and $B$. We first quote a well known fact, which has been in the literature since “generic projections” in [6], recorded as Lemma 3 in [19].

**Lemma 19.** Let $A \subseteq \mathbb{F}_p$ with $|A| > p^{1/2}$. Then

$$\sum_{x \in \mathbb{F}_p^*} E^+(A, xA), \sum_{x \in \mathbb{F}_p^*} E^x(A, x + A) \ll |A|^4.$$

Heuristically the above statement means that knowing, say $a, b, a', b'$ in the equation $a(b - x) = a'(b' - x)$ generically defines $x$, the constraint $|A| > p^{1/2}$ taking care of degeneracies. So the latter $\ll$ estimate is, in fact, an asymptotic identity.

Besides, by Cauchy-Schwarz, for every $x \in \mathbb{F}_p^*$ we have

$$E^+(A, xA), E^x(A, x + A) \geq |A|^4/p. \tag{29}$$

Indeed, we simply use $p$ as the upper bound for, say $|A + xA|$.

Combining the formula (28) – where we set $E^x(B, x + B) = (E^x(B, x + B) - |B|^4/p) + |B|^4/p$ and similarly for $E^+(C, xC)$ – with Lemma 19 we have, assuming
$|A| > p^{1/2}$ and using the Hölder inequality we obtain:

(30)

$$E \ll \frac{|A|^8}{p} + \sum_{x \neq 0} \left( E^+(C, xC) - \frac{|C|^4}{p} \right) \left( E^+(B, x + B) - \frac{|B|^4}{p} \right) \left( \sum_{x \neq 0} \left( E^x(B, x + B) - \frac{|B|^4}{p} \right)^{5/2} \right)^{2/5}.$$ 

The choice of exponents in the Hölder inequality has been made to conform with the estimate (5) in the sequel.

The main part of the argument is the following proposition, an analogue of Proposition 8 in [19].

**Proposition 20.** Let $A \subseteq \mathbb{F}_p$, with $p^{1/2} < |A| \leq p^{2/3}$ and $s \in (0, 3)$. Then

$$\sum_{x \neq 0} \left( E^+(A, xA) - \frac{|A|^4}{p} \right)^{1+s} = O \left( p^{1-\frac{1}{3}s} E^+(A)^{\frac{2}{3}+\frac{4}{3}s} \right)$$

and

$$\sum_{x \neq 0} \left( E^x(A, x + A) - \frac{|A|^4}{p} \right)^{1+s} = O \left( p^{1-\frac{1}{3}s} E^x(A)^{\frac{2}{3}+\frac{4}{3}s} \right).$$

Proposition 20 relies on the following lemma, the analogue of Theorem 2 in [19], which follows from Theorem 3.

**Lemma 21.** Let $A \subseteq \mathbb{F}_p$, $X \subseteq \mathbb{F}_p^*$. Suppose $|X| = O(|A|^2)$ and $|A|^2 |X| = O(p^2)$. Then

$$\sum_{x \in X} E^+(A, xA) \ll E^+(A)^{1/2} |A|^{3/2} |X|^{3/4}$$

and

$$\sum_{x \in X} E^x(A, x + A) \ll E^x(A)^{1/2} |A|^{3/2} |X|^{3/4}.$$ 

To keep the exposition more self-contained we sketch the proof of Lemma 21 dealing with its second estimate: the first one was the result of Theorem 2 in [19], and the two proofs are in essence identical.

**Proof.** (Sketch of proof.) Let $Y = \sum_{x \in X} E^x(A, x + A)$, that is the number of solutions of the equation

$$a(x + b) = c(x + d) : x \in X, a, b, c, d \in A.$$ 

It is easy to see that the condition $|X| = O(|A|^2)$ implies that the number of trivial solutions of the last equation (e.g. $a = c = 0$ and $x, b, d$ are any or $x = -b, c = 0$ and $a, d$ are arbitrary) is negligible. Rearranging and applying Cauchy-Schwarz we get $Y \ll (E^x(A)Z)^{1/2}$, where $Z$ is the number of solutions of the equation

$$\frac{x + b}{x + d} = \frac{x' + b'}{x' + d'} : x, x' \in X, b, d, b', d' \in A.$$
The number of nontrivial solutions of the latter equation can be estimated by using Theorem 19 in [1], which is a particular case of Theorem 3. This was done, in particular, in the proof of Corollary 8 of the latter paper. We nonetheless briefly show how.

Consider a family of planes in \( \mathbb{F}_p^3 \) with equations, in coordinates \((x_1, x_2, x_3)\) not to be confused with \(x, x' \in X\), as follows:

\[
\frac{1}{x + d} x_1 - x_2 - b' x_3 + \frac{x}{x + d} = 0,
\]

and their incidences with points \((x_1, x_2, x_3) = (b, x', x' + d, 1)\). It is easy to verify, see [1], that there are \(m = |X||A|^2\) planes and points. The constraints of Lemma 21 ensure that the main term \(m^{3/2}\) dominates in the estimate Theorem 3 and the theorem is applicable. Thereupon, the second estimate of Lemma 21 follows. □

**Remark 3.** Using methods from [18] (see the proofs of Lemmas 2.3, 2.4) one can prove another variant of Lemma 21, namely, for any \(A \subseteq \mathbb{F}_p\) and \(X \subseteq \mathbb{F}_p^*\) with \(|A| \leq p^{2/3}\) the following holds

\[
\sum_{x \in X} E^+(A, x A) \ll |A|^{13/4} |X|^{1/2},
\]

and

\[
\sum_{x \in X} E^\times(A, x + A) \ll |A|^{13/4} |X|^{1/2}.
\]

Lemma 21 can be restated in the standard way, similar to the well-known restatement of the Szemerédi-Trotter theorem, Theorem 2 here, as \(O\left(\frac{n^2}{\tau^3} + \frac{n}{\tau}\right)\) as the upper bound on the number of \(\tau\)-rich lines. See Lemma 4 of [19]. We quote an auxiliary Lemma from [22] which appears (and is proved) explicitly in [19]:

**Lemma 22.** For every set \(X \subseteq \mathbb{F}_p^*\) we have the following inequality

\[
\sum_{x \in X} \left( E^+(A, x A) - \frac{|A|^4}{p} \right), \sum_{x \in X} \left( E^\times(A, x + A) - \frac{|A|^4}{p} \right) \leq p |A|^2.
\]

**Lemma 23.** Let \(A \subseteq \mathbb{F}_p\), \(|A| > p^{1/2}\) and \(1 \leq K \leq p^{E^+(A)/2|A|\tau}\).

Then the number of \(x \in \mathbb{F}_p^*\) such that \(E^+(A, x A) > \frac{E^+(A)}{K}\) is \(O\left(K^4 \frac{|A|^6}{E^+(A)^2}\right)\). A similar bound holds for the number of \(x \in \mathbb{F}_p^*\) such that \(E^+(A, x + A) > \frac{E^\times(A)}{K}\).

**Proof.** Note that \(K\) is well defined, by (29). Let \(X\) be the set of \(x\) in question. Firstly we show that \(|A|^2|X| = O(p^2)\). From Lemma 22 we know that

\[
p |A|^2 \geq \sum_{x \in X} \left( E^+(A, x A) - \frac{|A|^4}{p} \right) \geq \sum_{x \in X} \left( \frac{E^+(A)}{K} - \frac{|A|^4}{p} \right).
\]

Hence we have

\[
p |A|^2 \geq |X| \left( \frac{E^+(A)}{K} - \frac{|A|^4}{p} \right).
\]
and because of our choice of $K$, the first term dominates. So $|X| \leq \frac{2p|A|^2K}{E^+(A)}$; substitution yields $|A|^2|X| = O(p^2)$ and $|X| = O(|A|^2)$.

Next, we use Lemma 23 to obtain

$$\sum_{x \in X} E^+(A, xA) = O(E^+(A)^{1/2}|A|^{3/2}|X|^{3/4}).$$

All that remains is to evaluate the following:

$$\frac{|X|E^+(A)}{K} \leq \sum_{x \in X} E^+(A, xA) = O(E^+(A)^{1/2}|A|^{3/2}|X|^{3/4}).$$

One rearranges to obtain the desired bound on $|X|$. The multiplicative energy case is identical. □

Thus we pass from having to satisfy the conditions of Lemma 23 to meeting those of Lemma 22. We now prove Proposition 20 as the proofs for both statements are the same, we prove the first one only.

Proof of Proposition 20. Note that by Cauchy-Schwarz, for every $x \neq 0$, we have $E^+(A, xA) \leq E^+(A)$.

Set $M = (pE^+(A)/8|A|^4)^{1/3}$, so $1/2 \leq M \leq pE^+(A)/(2|A|^4)$ by (29). Since also $p^{1/2} < |A| < p^{2/3}$, for any $1 \leq K \leq M$ the conditions of Lemma 22 are satisfied.

For ‘small’ energies when $E^+(A, xA) \leq E^+(A)/M$, we rely on (29) which ensures no sign alterations and proceed with a trivial inequality and Lemma 22 to obtain:

$$\sum \left( E^+(A, xA) - \frac{|A|^4}{p} \right)^{1+s} \leq \sum \left( \frac{E^+(A)}{M} \right)^s \left( E^+(A, xA) - \frac{|A|^4}{p} \right)$$

$$\leq p|A|^2 \left( \frac{E^+(A)}{M} \right)^s,$$

where both sums are taken over the set $\{x \neq 0 : E^+(A, xA) \leq E^+(A)/M\}$. Note that if $M < 1$ then the inequalities $E^+(A, xA) - \frac{|A|^4}{p} \leq E^+(A, xA) \leq E^+(A)/M$ hold by trivial reasons.

For ‘large’ $E^+(A, xA)$ we use Lemma 23 and a dyadic argument. Let

$$X_i := \{x : 2E^+(A)/M < E^+(A, xA) \leq \min(2^{i+1}E^+(A)/M, E^+(A))\}.$$

For $0 \leq i \ll \log M$, set $2^{-i}M = K_i$, so $1 \leq K_i \leq M$.

By Lemma 23 we know that $|X_i| = O\left(2^{-4i}M^i|A|^6\right)/E^+(A)^{1-s}$). So

$$\sum_{E^+(A, xA) > E^+(A)/M} \left( E^+(A, xA) - \frac{|A|^4}{p} \right)^{1+s} \leq \sum_i \sum_{x \in X_i} E^+(A, xA)^{1+s}$$

$$\ll \sum_i |X_i|E^+(A)^{1+s}2^{(1+s)i}M^{-(1+s)}$$

$$\ll \frac{M^{3-s}|A|^6}{E^+(A)^{1-s}}.$$
Here we have used that \( s \in (0, 3) \) to sum the geometric progression in \( i \), so the constant hidden in the last inequality depends on \( s \). In view of the choice of \( M \), independent of \( s \), the latter two estimates match, concluding the proof of Proposition \( \ref{prop:} \) \( \square \)

To conclude the proof of Theorem \( \ref{thm:} \) we observe that by Proposition \( \ref{prop:} \) applied to the estimate \( \ref{est:} \) we have

\[
\mathcal{E} \ll |A|^8/p + p^{2/3}|A|^{10/3} |E^+(C)| E^+(B)^{3/2} |A|^{4/15},
\]

given that \(|A| \leq p^{3/5}\). Applying \( \ref{est:} \) of Corollary \( \ref{cor:} \) (with the notations \( B \) and \( C \) reversed) it is immediate to conclude that the first term in the estimate dominates if \(|A| \geq p^{25/42} \log^K |A| \), where \( K \) depends only on the power of \( \log |A| \) hidden in the estimate \( \ref{est:} \). Note that \( 25/42 < 3/5 \), so the upper bound on \(|A|\) to make Corollary \( \ref{cor:} \) applicable has been satisfied.

For such \( A \) the number of solutions of equation \( \ref{eq:} \) is \( O(|A|^8/p) \), which completes the proof of Theorem \( \ref{thm:} \) \( \square \)

7. PROOF OF THEOREM \( \ref{thm:} \) AND ENSUING STATEMENTS

We prove Theorem \( \ref{thm:} \)

**Proof.** Let \( E = E^+(A) \geq |A|^3/K \). Put \( A_s = A \cap (A - s) \). We have

\[
(32) \quad E = \sum_{s \in G} |A_s|^2 = \sum_s \sum_{x, y} A_s(x)A_s(y) = \sum_s \sum_{x, y} A(x)A(y)A(x + s)A(y + s).
\]

Let \( \varepsilon \in (0, 1) \) be a real number which we will choose later. Let us put

\[
P = P_\varepsilon = \left\{ s : |A_s| \geq \varepsilon |A| \right\} / 2K.
\]

Clearly, the set \( P_\varepsilon \) is symmetric for any \( \varepsilon \) and \( |P_\varepsilon| \leq 2K\varepsilon^{-1}|A| \). As

\[
\sum_s \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y) = \sum_{x \neq y \in P_\varepsilon} A(x)A(y)|A_{x - y}| < \varepsilon |A|^3 / 2K,
\]

then by combining the last estimate with \( \ref{est:} \), we get

\[
\sum_{s : |A_s| \geq |A|/2K} \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y) > \varepsilon \sum_{s : |A_s| \geq |A|/2K} \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y).
\]

It follows that there is \( s \) with \(|A_s| \geq |A|/(2K)\) satisfying,

\[
\varepsilon \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y) > \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y).
\]

In other words

\[
(33) \quad \sum_{x \neq y \in P_\varepsilon} A_s(x)A_s(y) > (1 - \varepsilon)|A_s|^2.
\]
Now let us consider a non–oriented graph (with loops) $\mathcal{G} = (V, E)$ with the vertex set equal to $A_s$ such that its vertices $x, y$ are connected iff $x − y \in P_{\varepsilon}$. It is easy to see from (38) that $|E| \sim (1 − \varepsilon)|A_s|^2$. Put

$$A_s = \{ v \in V : \deg v \geq (1 − 2\varepsilon)|V| \} \subseteq A_s.$$ 

Inequality (38) implies $|A_s| \geq \varepsilon|V| \geq \varepsilon|A|/(2K)$. Moreover for any vertices $a_1, \ldots, a_k \in A_s$ there are at least $\varepsilon\sum_{j=1}^{k} |V|$ common neighbours $x \in V$; i.e. vertices $x$ such that $(a_1, x), \ldots, (a_k, x) \in E$. By putting $\varepsilon = 1/(4k)$, we obtain the result. 

Theorem [14] enables one to achieve Balog-Wooley type decomposition results, dealing with the energies directly.

Proof. (Sketch of proof of Proposition [15])

Set $E^+(A) = |A|^3/K$. Using Theorem [14] in multiplicative form with $k = 2$, we find a set $A_s \subseteq A, |A_s| \gg |A|/K$ and a set $P \subseteq A/A, |P| \ll K|A|$ such that for any $a, b \in A_s$, the following holds $|A \cap aP \cap bP| \gg |A|/K$. Thus $E^+(A_s)$ is bounded from above by

$$O\left(|A|^2 \sum \{ (a p_1^{-1} + p_2^{-1}) : p_1, p_2, p_3, p_4 \in P, a, b \in A \} \right).$$

Using a consequence of the Szemerédi–Trotter theorem, see e.g. Lemma 2.5 from [18], we get

$$E^+(A_s) \ll |A|^2 \cdot (E^+(A))^{1/2} |P|^3 \ll K^5 |A| (E^+(A))^{1/2}.$$ 

This completes the proof. 

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, I.D. Shkredov, Growth estimates in positive characteristic via collisions, Int Math Res Notices (2016), doi: 10.1093/imrn/rnw206.
[2] A. Balog, T.D. Wooley, A low–energy decomposition theorem, Quarterly Journal of Mathematics, 68:1 (2017), 207–226, doi: 10.1093/qmath/haw023.
[3] J. Bourgain, More on the sum–product phenomenon in prime fields and its applications, International Journal of Number Theory 1:1 (2005), 1–32.
[4] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, Geom. Funct. Anal., 18 (2009), 1477–1502.
[5] J. Bourgain, M.Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, Math. Proc. Cambridge Philos. Soc. 146:1 (2009), 1–21.
[6] J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields, and applications, Geom. Funct. Anal. 14 (2004), 27–57.
[7] J. Chapman, M.B. Erdőc, D. Hart, A Iosevich, D. Koh, Pinned distance sets, $k$-simplices, Wolff’s exponent in finite fields and sum-product estimates, Mathematische Zeitschrift 271:1-2 (2012), 63–93.
[8] G. Elekes, On the number of sums and products, Acta Arith. 81 (1997), 365–367.
[9] G. Elekes, I. Z. Ruzsa, Few sums, many products, Studia Sci. Math. Hungar. 40:3 (2003), 301–308.
[10] P. Erdős, E. Szemerédi, On sums and products of integers, Studies in pure mathematics, 213–218, Birkhäuser, Basel, 1983.
[11] K. Ford, The distribution of integers with a divisor in a given interval, Annals of Math., 168 (2008), 367–433.
[12] W.T. Gowers, A new proof of Szemerédi’s theorem, Geom. Funct. Anal. 11 (2001), 465–588.
B. Green, T. Tao, *On Sets Defining Few Ordinary Lines*, Discrete & Computational Geometry 50:2 (2013), 409–468.

T.G.F. Jones, O. Roche-Newton, *Improved bounds on the set A(A + 1)*, J. Combin. Theory Ser. A 120:3 (2013), 515–526.

S.V. Konyagin, M. Rudnev, *On new sum-product-type estimates*, SIAM J. Discrete Math. 27:2 (2013), 973–990.

S.V. Konyagin, I.D. Shkredov, *On sum sets of sets, having small product sets*, Proc. Steklov Inst. Math., 3:290, (2015), 304–316.

S.V. Konyagin, I.D. Shkredov, *New results on sum–products in R*, Proc. Steklov Inst. Math., 294:78, (2016), 87–98.

B. Murphy, O. Roche–Newton, I.D. Shkredov, *Variations on the sum-product problem*, SIDMA, 29:1 (2015), 514–540.

G. Petridis, *Products of Differences in Prime Order Finite Fields*, arXiv:1602.02142 [math.CO] 5 Feb 2016.

O. Roche-Newton, M. Rudnev, I. D. Shkredov, *New sum-product type estimates over finite fields*, Adv. Math. 293 (2016), 589–605.

M. Rudnev, *On the number of incidences between planes and points in three dimensions*, Combinatorica (2017), 1–36, doi:10.1007/s00493-016-3329-6.

T. Schoen, *New bounds in Balog–Szemerédi–Gowers theorem*, Combinatorica, 34:5 (2014), 1–7.

T. Schoen, I.D. Shkredov, *Higher moments of convolutions*, J. of Number Theory, 133 (2013), 1693–1737.

I.D. Shkredov, *On sums of Szemerédi–Trotter sets*, Proc. Steklov Inst. Math., 289, (2015), 300–309.

I.D. Shkredov, *Difference sets are not multiplicatively closed*, Discrete Anal., 17 (2016), 1–21, doi: 10.19086/da.913.

I.D. Shkredov, *Some remarks on the Balog–Wooley decomposition theorem and quantities D+, D*, Proc. Steklov Inst. Math., accepted, arXiv:1605.00266v1 [math.CO] 1 May 2016.

J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. 37: 4 (2005), 491–494.

J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math. 222: 2 (2009), 402–408.

S. Stevens, F. de Zeeuw, *An improved point-line incidence bound*, arXiv: 1609.06284v2 [math.CO] 7 Oct 2016.

E. Szemerédi, W. T. Trotter, *Extremal problems in discrete geometry*, Combinatorica 3 (1983), 381–392.

T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press (2006).

C. Tóth, *The Szemerédi–Trotter theorem in the complex plane*, Combinatorica 3 (2015), no 1, 95–126.

**Misha Rudnev**, Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

*E-mail address: m.rudnev@bristol.ac.uk*

**Ilya D. Shkredov**, Steklov Mathematical Institute, Division of Number Theory, ul. Gubkina, 8, Moscow, 119991; IITP RAS, Bolshoy Karetny per. 19, Moscow, 127994 and MIPT, Institutskii per. 9, Dolgoprudni, 141701

*E-mail address: ilya.shkredov@gmail.com*

**Sophie Stevens**, Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

*E-mail address: sophie_ccs.2011@bristol.ac.uk*