JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Brendan MURPHY, Misha RUDNEV, Ilya SHKREDOV et Yuri SHTEINIKOV

On the few products, many sums problem

Tome 31, n° 3 (2019), p. 573-602.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_3_573_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 573–602

On the few products, many sums problem

par Brendan MURPHY, Misha RUDNEV, Ilya SHKREDOV et Yuri SHTEINIKOV

Résumé. Nous prouvons de nouvelles estimations quantitatives pour les propriétés additives des ensembles finis à doublement multiplicatif petit $|AA| \leq M|A|$ dans la catégorie des ensembles réels ou complexes A, ainsi que pour les sous-groupes du groupe multiplicatif d'un corps fini premier. Ces améliorations reposent sur de nouveaux lemmes combinatoires qui peuvent présenter un intérêt indépendant.

Dans le cas réel,nos principaux résultats sont l'inégalité

$$|A-A|^3|AA|^5 \gtrsim |A|^{10}$$

qui redistribue les exposants dans l'inégalité somme-produit d'Elekes et la nouvelle borne pour l'énergie additive

$$\mathsf{E}(A) \lesssim_M |A|^{49/20},$$

qui améliore les résultats précédemment connus et s'accorde, au sens expliqué dans l'article, avec la meilleure borne connue pour l'ensemble somme $|A+A| \gtrsim_M |A|^{8/5}$.

Ces bornes, avec $M=1$, s'appliquent également aux sous-groupes multiplicatifs de $\mathbb{F}_p^\times$ d'ordre $O(\sqrt{p})$. Nous adaptons la borne pour l'énergie citée ci-dessus à des sous-groupes plus grands et obtenons de nouvelles bornes pour les écarts entre les éléments dans les classes des sous-groupes d'ordre $\Omega(\sqrt{p})$.

Abstract. We prove new quantitative estimates on additive properties of finite sets A with small multiplicative doubling $|AA| \leq M|A|$ in the category of real/complex sets as well as multiplicative subgroups in the prime residue field. The improvements are based on new combinatorial lemmata, which may be of independent interest.

Our main results are the inequality

$$|A-A|^3|AA|^5 \gtrsim |A|^{10},$$

over the reals, "redistributing" the exponents in the textbook Elekes sum-product inequality and the new best known additive energy bound $\mathsf{E}(A) \lesssim_M$

Manuscrit reçu le 24 avril 2018, révisé le 5 septembre 2019, accepté le 28 septembre 2019.
2010 *Mathematics Subject Classification.* 11B13, 11B50, 11B75.
Mots-clefs. Sum–product phenomenon, multiplicative subgroups, additive energy.
We thank O. Roche-Newton, J. Solymosi, S. Stevens and D. Zhelezov for their advise on the exposition of the results in this paper. The third author is supported by the Russian Science Foundation under grant 19–11–00001.

$|A|^{49/20}$, which aligns, in a sense to be discussed, with the best known sum set bound $|A+A| \gtrsim_M |A|^{8/5}$.

These bounds, with $M=1$, also apply to multiplicative subgroups of $\mathbb{F}_p^\times$, whose order is $O(\sqrt{p})$. We adapt the above energy bound to larger subgroups and obtain new bounds on gaps between elements in cosets of subgroups of order $\Omega(\sqrt{p})$.

1. Introduction

Let A be a finite set in a field. We use the standard notation $A \pm A$, AA, A/A for the sets of all sums, differences, products and finite ratios of pairs of elements of A, as well as A^{-1} for the set of inverses, $A+a = A+\{a\}$ for translates, etc. By A^k, however, we mean the k-fold Cartesian project of A with itself.

The Erdős–Szemerédi [10] or sum-product conjecture applied to reals challenges one to prove that $\forall\, \epsilon > 0$,

$$|AA| + |A+A| \geq |A|^{2-\epsilon}, \tag{1.1}$$

for all sufficiently large $A \subset \mathbb{R}$.

The *weak Erdős–Szemerédi conjecture*, or *few products, many sums* is a claim that if A has small multiplicative doubling, that is $|AA| \leq M|A|$ for some $M \geq 1$, then $|A \pm A| \gtrsim_M |A|^2$, where the inequality symbols $\gtrsim_M, \lesssim_M$ will subsume universal constants, powers of $\log|A|$ (logarithms are meant to be base 2) and powers of M if the subscript $_M$ is present; constants alone are suppressed by the standard Vinogradov notation $\ll, \gg$ and, respectively O, Ω (as well as $\approx$ for both O and Ω); these can also be subscripted by $_M$ to hide powers of M. When both $\lesssim$ and $\gtrsim$ bounds hold we may use the symbol $\sim$. To ensure not dividing by zero, it is assumed by default in all formulations that $|A| > 1$ as well as $0 \notin A$.

In this paper we address the case $A \subset \mathbb{R}$ as well as when A is a multiplicative subgroup of the multiplicative group $\mathbb{F}_p^\times$ of the prime residue field $\mathbb{F}_p$. All our results over the reals apply to the complex field as well: we do not make a distinction and *real* may be read in the sequel as *real or complex*.

The weak Erdős–Szemerédi conjecture appears to be the key issue in understanding the more general sum-product phenomenon, see e.g. a survey [11] and the references therein. If in its above formulation one allows exponential dependence on M, the affirmative answer was established by Chang and Solymosi [4] via a variant of Schmidt's subspace theorem.

The strongest few products, many sums result known so far is due to by Bourgain and Chang [2] in the context of integers (rationals), the proof relying strongly on the main theorem of arithmetics. It claims that for any $\epsilon > 0$, there is a power $C(\epsilon)$, so that $|A \pm A| \gg M^{-C(\epsilon)}|A|^{2-\epsilon}$, although $C(\epsilon)$ goes to infinity as $\epsilon \to 0$.

Our results are somewhat different in flavour, for our dependence $C(\epsilon)$ is linear (as well as all the constants involved are "reasonable" and computable); what we cannot do is go below $\epsilon = 1/3$.

The converse question *few sums, many products* is resolved over the reals, where it was shown by Elekes and Ruzsa [9] to follow from the Szemerédi–Trotter theorem. Its strongest quantitative version is implied by Solymosi's [41] inequality $|AA||A+A|^2 \gtrsim |A|^4$, although this does not embrace $A - A$. Moreover, [27, Theorem 12] presents an affirmative quantitative estimate to an L^2-variant of the question. The few sums, many products question is not settled in positive characteristic, the best known results being [22, Theorem 2].

One can target various type of estimates along the lines of the few products, many sums — henceforth FPMS — phenomenon (the acronym is meant to embrace differences and ratios as well) in terms of the properties of the number of realisations function $r_{A\pm A}(x)$, namely

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

and its moments, in particular

$$\mathsf{E}(A) =: \sum_x r^2_{A\pm A}(x),$$

known as (additive) energy. Energy is independent of the choice of $\pm$, being the number of solutions of the equation $a_1 + a_2 = a_3 + a_4$, with variables in A, which can be rearranged. A fruitful viewpoint at looking at $r_{A-A}(x)$ is that x represents an equivalence class on $A \times A$ by translation, with $r_{A-A}(x)$ members.

The three types of FPMS bounds one may be interested in are as follows.

(i) *Convolution support:* inequalities $|A \pm A| \gg_M |A|^{2-\epsilon}$ aiming at $\epsilon \to 0_+$.

(ii) *Energy, or L^2-bounds:* inequalities $\mathsf{E}(A) \ll_M |A|^{2+\epsilon}$ aiming at $\epsilon \to 0_+$.

(iii) *L^∞-bounds:* inequalities $r_{A+A}(x) \ll_M |A|^\epsilon$, aiming at $\epsilon \to 0_+$, same for $r_{A-A}(x)$ for $x \neq 0$.

Energy bounds clearly imply ones for support: by the Cauchy–Schwarz inequality

$$|A \pm A| \geq \frac{|A|^4}{\mathsf{E}(A)}\,.$$

As far as the last question is concerned, there is a bound $O(|A|^{2/3})$ implied by a single application of the Szemerédi–Trotter theorem; nothing better appears to be known, and we therefore do not pursue the issue any further.

Thus this paper addresses questions (i) and (ii). Techniques available today have limited powers, and those in this paper prefer differences to sums, owing to shift invariance.

Let us give a brief outline of how results of this paper fit into the general state of the art. The starting point to this line of work was the paper of Elekes [7]. It implies (although only question (i) was addressed) that $\mathsf{E}(A) \ll M|A|^{5/2}$, see (2.4) below. A similar bound, with $M = 1$, is implicit in the paper Elekes, Nathanson and Rusza [8] on sumsets of convex sets ([8] also addressed question (i)). Both bounds arise from an application of the Szemerédi–Trotter theorem, made possible by a trick of adding an extra variable, owing to associativity, much in the way this is done in the well-known Ruzsa distance inequality, see e.g. [45]. These works established what we refer to as the *threshold* value of $\epsilon = 1/2$.

Schoen and the third author [28] succeeded in decreasing the value of ϵ apropos of the analogue of question (i) in the *convex set* setting, having introduced the concept and taken advantage of combinatorics arising in the context of the third moment, alias cubic energy $\mathsf{E}_3(A)$ (see (2.1) below), which has played a key role in quantitative estimates, both in the convex sumset and sum-product type settings, ever since, including this paper. The key issue is that the Szemerédi–Trotter theorem yields a very strong estimate (2.4) for $\mathsf{E}_3(A)$, (with $M = 1$ in the convex set case). Li [17] observed that the analysis of [28] could be adapted to the FPMS case: this with further generalisations was the subject of his paper with Roche-Newton [18].

Energy bounds, concerning question (ii), are harder to establish, and in order to improve the threshold exponent $5/2$ (which applies in a broad context, see [25]) the third author set forth in [31] an eigenvalue technique, which was then further developed in [30], [32], [33]. In the latter paper [33, Theorem 6.1] it was shown that, in fact, the estimates (2.4) for $\mathsf{E}(A)$ and $\mathsf{E}_3(A)$ effect a certain *critical relation* between the two quantities, which guarantees sub-threshold improvement of the estimate for $\mathsf{E}(A)$ — question (ii) and therefore question (i) — via the Balog–Szemerédi–Gowers theorem. However, the quantitative improvement this way, although very general and valid also in non-commutative context, is quite small. The eigenvalue method yields stronger results, being able to reach to the multiplicative properties of A in the FPMS case more explicitly. For an exhaustive exposition of the eigenvalue method see [33, Section 4].

The aim of this paper is to prove the strongest so far quantitative bounds on questions (i) and (ii) in the FPMS case, which explore the multiplicative structure of A more thoroughly and in particular do not extend (at least we do not see how) to the convex set case. Our first result is bringing ϵ down to $1/3$ for the size of $A - A$ in Theorem 1.3.

However, we are quite far from being able to bring ϵ from $1/2$ down to $1/3$ as to the energy estimate in question (ii) and even the cardinality of $A + A$ in question (i). We can only decrease $\epsilon = 1/2$ by $1/20$ and $1/10$

(rather by 1/6) respectively. The new best known bond for additive energy, stated in Theorem 1.4 is due to Lemma 4.1, which is very specific to the FPMS case.

The bound $|A+A| \gtrsim_M |A|^{8/5}$ following from Theorem 7.1 in the last section of the paper has already been established by the third author in [32]. We include that section, owing to the better M-dependence in the estimate of the theorem, whose proof is based, in particular, on a new energy pigeonholing Lemma 7.2 that we feel may be useful for other purposes. Until recently, results of the type that the lemma presents were drawn using the quantitatively costly Balog–Szemerédi–Gowers theorem. We also remark that if we could improve the key estimate (4.8) in the proof of the energy Theorem 1.4, this would also improve the sum set exponent 8/5.

As some consolation, as well as possibly a principle obstacle against improving the estimates in this paper, given the technique, we take the example by Balog and Wooley [1], also discussed in [27], which shows that generally the exponent 7/3 is the best possible one for energy inequalities: there are sets A, such that any positive proportion subset $A' \subseteq A$ would have both $\mathsf{E}(A)$ and its multiplicative analogue exceeding $|A|^{7/3}$. This is unlikely to happen in the extremal FPMS case but nonetheless, together with the results in this paper bears some evidence that one can hardly expect to be able to establish L^2-estimates, which would be equally strong to support ones; certainly this is the case within the applicability of the techniques we possess. In fact, the methods in this paper are essentially *energy methods*, that is the multiplicative constant M can be viewed as equal to $|A|^3/\mathsf{E}^\times(A)$, where $\mathsf{E}^\times(A)$ is multiplicative energy, and the key estimates, with some work, can be re-cast in terms of the Balog–Wooley decomposition set forth in [1], using the state-of-the-art techniques, developed in [27].

1.1. Background and main results. Our key geometric tool is the Szemerédi–Trotter theorem [44].

Theorem 1.1. *Consider a set of n points in $\mathbb{R}^2$. Connect all pairs of distinct points by straight lines, then for $k \geq 2$, the number of lines supporting at least k points is*

$$O\left(\frac{n^2}{k^3} + \frac{n}{k}\right). \tag{1.2}$$

The total number of incidences between n points and m straight lines is $O(m^{2/3}n^{2/3} + m + n)$.

In fact, in our applications the point set is a Cartesian product. In this case there is an easier proof of estimate (1.2) by Solymosi and Tardos [42], in particular the hidden constants having very reasonable values in both the real and complex settings.

Heath-Brown and Konyagin [12] used the Stepanov method to prove a quantitatively similar result about multiplicative subgroups in $\mathbb{F}_p^\times$. This was further developed in [21], [38], the statement we quote can be found in [21].

Theorem 1.2. *Let Γ be a multiplicative subgroup in $\mathbb{F}_p^\times$ and $\Theta \subset \mathbb{F}_p^\times/\Gamma \times \mathbb{F}_p^\times/\Gamma$, $|\Gamma|^4|\Theta| < p^3$ and $|\Theta| \leqslant 33^{-3}|\Gamma|^2$. Then*

$$\sum_{(u,v)\in\Theta} \Big|\{(x,y) \in \Gamma \times \Gamma : ux + vy = 1\}\Big| \ll (|\Gamma||\Theta|)^{2/3}\,. \tag{1.3}$$

We observe, and will use, the heuristic fact that both Theorem 1.1 and 1.2 would yield the same main factor in the upper bound $(|X||Y||Z||\Gamma|)^{2/3}$ — see e.g. [38, Corollary 5.1] — for the number of solutions of the equation $ax + y = z$, with $a \in \Gamma$ and $x \in X$, $y \in Y$, $z \in Z$, with the restriction in $\mathbb{F}_p$ that the sufficiently small in terms of p sets X, Y, Z be Γ-invariant — that is, say $X\Gamma = X$ — and extra polynomial dependence in M in the real case. For some recent work along the same lines on multiplicative subgroups in $\mathbb{F}_p$ see, e.g., [20], [35], [37] and the references contained therein.

Applications of the Szemerédi–Trotter theorem to sum-product type problems were, as we already said, started by Elekes [7], who proved the textbook inequality

$$|A \pm A|^2|AA|^2 \gg |A|^5, \tag{1.4}$$

which established the threshold FPMS inequality $|A \pm A| \gg_M |A|^{3/2}$.

Developing more efficient applications of the Szemerédi–Trotter theorem to the FPMS question together with arithmetic/analytic combinatorics lemmata has been the subject of much recent work: see, e.g. [23], [27], [30], [32], [36], [39] (and the references therein).

In particular, the third author [36] established the inequality

$$|A - A|^6|AA|^{13} \gtrsim |A|^{23}. \tag{1.5}$$

(In the statement of the corresponding [36, Theorem 1] one has the ratio set A/A, but after some inspection of the proof can be extended to embrace AA as well.) Inequality (1.5) sets the world record $|A - A| \gtrsim_M |A|^{5/3}$, which we believe is unlikely to be beaten within the current state of the art. Similarly the inequality $|\Gamma \pm \Gamma| \gg |\Gamma|^{3/2}$ for a multiplicative subgroup $\Gamma \subset \mathbb{F}_p$, with $|\Gamma| \leq p^{2/3}$, was established by Heath-Brown and Konyagin [12] and improved to $|\Gamma - \Gamma| \gtrsim |\Gamma|^{5/3}$ for $|\Gamma| \leq \sqrt{p}$ in [38].

On the other hand, back to the real case, in the sense of the original question (1.1), that is when cardinalities $|AA|$ and $|A - A|$ are roughly the same, inequality (1.5) is weaker that (1.4).

The first inequality in the statement of the following theorem strengthens the inequality (1.5) (modulo the power of $\log|A|$) so that it matches the Elekes one, involving the difference set in the case of similar cardinalities.

Theorem 1.3. *For a real set A*

$$|A-A|^3|AA|^5 \gg \frac{|A|^{10}}{\log^{1/2}|A|}. \tag{1.6}$$

We remark that in estimates (1.6) one can replace AA with A/A. The proof also applies, with $AA = A$, to the case when A is replaced by a multiplicative subgroup $\Gamma \subset \mathbb{F}_p^\times$, with $|\Gamma| \leq \sqrt{p}$. In the latter case the inequality is due to the third author and Vyugin [38].

The next theorem is an L^2 estimate in the following Theorem 1.4. It improves the previously best known bound $\mathsf{E}(A) \lesssim_M |A|^{32/13}$ in [32, Theorem 8] and [33, Theorem 5.4]. The improvement is largely due to the forthcoming Lemma 4.1.

Theorem 1.4. *Let $A \subset \mathbb{R}$ and $|AA| \leqslant M|A|$. Then*

$$\mathsf{E}(A) \ll M^{8/5}|A|^{49/20}\log^{1/5}|A|\,. \tag{1.7}$$

The same estimate, with $M = 1$ holds for a multiplicative subgroup $\Gamma \subset \mathbb{F}_p^\times$, with $|\Gamma| \leq \sqrt{p}$.

L^2-estimates represent much interest as to many questions, arising in the context of multiplicative subgroups in $\mathbb{F}_p$. Our new energy bound brings an improvement to several such bounds in the literature. We develop some applications in Section 6. The main result in Section 6 is Theorem 6.8, yielding progress on the question of maximum gap size between coset elements, introduced by Bourgain, Konyagin and Shparlinski in [3].

In conclusion of this section we remark that all the known proofs of the Szemerédi–Trotter theorem strongly rely on order properties of reals, and despite recent progress in incidence theory over general fields (see [26], [43]) the versions of the Szemerédi–Trotter theorem which apply there are weaker than Theorem 1.1. On a somewhat pessimistic note, it appears extremely unlikely that the weak Erdős–Szemerédi conjecture can be resolved over the reals without a novel insight that we currently do not possess. In particular, inequality (1.6), its proof being simple as it is, appears to be the best one can hope for within today's scope of ideas.

2. The cubic energy: basic lemmata

In this short section we re-introduce the concept of cubic energy $\mathsf{E}_3(A)$, namely the third moment of the number-of-realisations function r_{A-A}. Generally, for $q > 1$ we define

$$\mathsf{E}_q(A) := \sum_d r_{A-A}^q(d), \tag{2.1}$$

omitting the subscript for $q=2$, where we also write $A_d = A\cap(A+d)$, as well as

$$\mathsf{E}(A,B)=\sum_d |A\cap(B+d)|^2.$$

Returning to (2.1) we are especially interested in the case $q=3$.

Notation-wise, if the domain of the summation index is not specified, this means the whole universe $\mathbb{R}$ or $\mathbb{F}_p$.

Geometrically $\mathsf{E}_3(A)$ is the number of collinear triples of points in the Cartesian product $A\times A\subset\mathbb{R}^2$ on unit slope lines $y=x+d$. By looking at the projections of such a collinear point triple on the coordinate exes, the same quantity can be re-counted as

$$\mathsf{E}_3(A)=\sum_{d,d'}|A\cap(A+d)\cap(A+d')|^2=\sum_{d'}\mathsf{E}(A,A_d)\,. \tag{2.2}$$

I.e., triples of elements $(a,b,c)\in A\times A\times A$ get partitioned into equivalence classes by translation, a single class being identified by differences $d=b-a$, and $d'=c-a$. Two latter triples of elements of A are equivalent if and only if they differ by translation. The quantity $\mathsf{E}_3(A)$ is the sum, over all equivalence classes, of squares of their population. (The same concerns the energy $\mathsf{E}(A)$, which pertains to equivalent by translation pairs, rather than triples, of elements of A.)

Note that since $b-c=d-d'$ is also a member of $A-A$, it follows by the Cauchy–Schwarz inequality that

$$|\{(d,d',d'')\in(A-A)^3:\,d''=d-d'\}|\ge\frac{|A|^6}{\mathsf{E}_3(A)}. \tag{2.3}$$

An application of Theorem 1.1 or Theorem 1.2 (see, e.g., [14, Lemma 7]) yields a near-optimal estimate for $\mathsf{E}_3(A)$ with $|AA|=M|A|$ or $A=\Gamma$, quoted as part of the following lemma.

Lemma 2.1. *Suppose $|AA|$ or $|A/A|=M|A|$. Then for any $A'\subseteq A$, and any B, one has bounds*

$$\mathsf{E}_3(A')\ll M^2|A'|^2|A|\log|A|,\qquad \mathsf{E}(A,B)\ll M|A||B|^{3/2}. \tag{2.4}$$

If Γ is a multiplicative subgroup in $\mathbb{F}_p^\times$, with size $O(\sqrt{p})$, and B a Γ-invariant set B, then

$$\mathsf{E}_3(\Gamma)\ll|\Gamma|^3\log|\Gamma|,\qquad \mathsf{E}(\Gamma,B)\ll|\Gamma||B|^{3/2}. \tag{2.5}$$

Besides, for $\Delta \ge 1$

$$\sum_{x:\, r_{A-A}(x)>\Delta} 1 \ll \frac{M^2|A|^3}{\Delta^3}, \qquad \sum_{x:\, r_{\Gamma-\Gamma}(x)>\Delta} 1 \ll \frac{|\Gamma|^3}{\Delta^3}, \tag{2.6}$$

$$\sum_{x:\, r_{A-A}(x)>\Delta} r^2_{A-A}(x) \ll \frac{M^2|A|^3}{\Delta}, \qquad \sum_{x:\, r_{\Gamma-\Gamma}(x)>\Delta} r^2_{\Gamma-\Gamma}(x) \ll \frac{|\Gamma|^3}{\Delta}. \tag{2.7}$$

Remark 2.2. In fact, as far as the multiplicative subgroup case is concerned, *all* the inequalities of Lemma 2.1 *but for* the second inequality in (2.5) are valid for $|\Gamma| \le p^{2/3}$. See, e.g., [34, Lemma 4]. This will be used in the proof of the forthcoming Theorem 6.5, where the second inequality in (2.5) will be replaced by Lemma 6.4.

We use Lemma 2.1 to immediately obtain the following consequence of estimate (2.3).

Corollary 2.3. *Under assumptions of Lemma 2.1,*

$$|\{(d,d',d'') \in (A-A)^3 :\, d''=d-d'\}| \gg \frac{|A|^3}{M^2 \log|A|},$$

and the same for Γ*, with* $M=1$.

3. Proof of Theorem 1.3

Let us first prove the inequality (1.6) under an additional easy-to-remove assumption. Define the set of popular differences as

$$P := \left\{ d \in A-A :\, r_{A-A}(d) \ge \left(\Delta := \frac{|A|^2}{2|A-A|}\right)\right\}. \tag{3.1}$$

By the pigeonhole principle

$$\sum_{d'\in P} r_{A-A}(d') \ge \frac{1}{2}|A|^2. \tag{3.2}$$

Proposition 3.1. *Suppose the bound of Corollary 2.3 applies to the equation* $d''=d-d'$*, with* $d,d'' \in A-A$ *and* $d' \in P$*. Then* (1.6) *follows.*

Proof. This becomes merely an application of the Szemerédi–Trotter theorem after for any $x \in A$ one writes

$$\begin{aligned} &|\{(d,d',d'') \in (A-A)\times P \times (A-A) :\, d=d'-d''\}| \\ &\quad = |\{(d,d',d'') \in (A-A)\times P \times (A-A) :\, d''=d-xd'/x\}| \\ &\quad \le \frac{1}{|A|}|\{(d,s,d'',x) \in (A-A)\times S \times (A-A)\times A :\, d''=d-s/x\}|, \end{aligned} \tag{3.3}$$

where

$$S := \{s \in AA-AA :\, r_{AA-AA}(s) \ge \Delta\}. \tag{3.4}$$

Indeed, since d' has at least Δ different representations $d' = b - a$ as a member of $A - A$, then xd' has at least Δ the representations in the form $xd' = xb - xa$ as the difference of two products from AA. It follows that

$$|S| \le \frac{(M|A|)^2}{\Delta}.$$

Thus the Szemerédi–Trotter theorem yields the upper bound for the number of solutions of the latter equation $d'' = d - s/x$, interpreted as incidences between $n = |A||A - A|$ points and $m = |S||A - A|$ lines, as

$$O\left(|A|^2 M^{4/3} |A - A|^{4/3} \Delta^{-2/3}\right) \tag{3.5}$$

(it is easy to see that if the term $|\mathcal{L}| = |A - A||S|$ were to dominate we would have a much better estimate than (1.6)).

Dividing this by $|A|$ in view of (3.3) and comparing this with the lower bound of Corollary 2.3 yields

$$\frac{|A|^3}{M^2 \log |A|} \ll |A| M^{4/3} |A - A|^2 |A|^{-4/3},$$

and hence (1.6).

It is easy to see, after trivial modifications of the argument involving M that wherever it appeared above, it could have as well come from $|A/A| = M|A|$. □

All it takes to ensure applicability of Proposition 3.1 is the following, essentially trivial lemma.

Lemma 3.2. *One has the following bound:*

$$\frac{|A|^6}{4} \le \mathsf{E}_3(A) |\{(d, d', d'') \in (A - A) \times P \times (A - A) : \, d'' = d - d'\}|.$$

Proof. The proof is just an application of the pigeonhole principle, often presented as a graph density argument. Considering P as a bipartite graph on $A \times A$, it has density $\ge 1/2$. Therefore, the number of triples (a, b, c) with $a - b \in P$ is $\ge |A|^3/2$. The claim of the lemma now follows by the Cauchy–Schwarz inequality, just like (2.3) above. □

4. Proof of Theorem 1.4

The proof of Theorem 1.4 mainly rests on lemmata 4.1 and 4.5.

In general, for $k \geqslant 2$ an integer, and A a subset of an abelian group, let $\mathsf{T}_k(A)$ (such additive characteristics of sets appear throughout additive combinatorics literature) be the quantity

$$\mathsf{T}_k(A) := |\{(a_1, \dots, a_k, a'_1, \dots, a'_k) \in A^{2k} : \, a_1 + \dots + a_k = a'_1 + \dots + a'_k\}|. \tag{4.1}$$

Clearly $\mathsf{T}_2(A) = \mathsf{E}(A)$ is additive energy; we here focus on $\mathsf{T}_3(A)$. We have also denoted by $\mathcal{T}(A)$ the number of *collinear point triples* in the plane set

$A \times A$. Note that Theorems 1.1 and 1.2, applied respectively in the real and $|\Gamma| \le \sqrt{p}$ multiplicative subgroup $\Gamma \subset \mathbb{F}_p^\times$ settings, ensure that

$$\mathcal{T}(A) \ll |A|^4 \log |A|. \tag{4.2}$$

The next lemma evinces a connection between the quantities $\mathsf{T}_3(A)$ and $\mathcal{T}(A)$.

Lemma 4.1. *One has the inequality*

$$\mathsf{T}_3(A) \leqslant \frac{|AA/A|}{|A|^2} \min\Big(|AA|\sqrt{\mathcal{T}(A/AA)\cdot\mathcal{T}(AA)},\ |A/A|\sqrt{\mathcal{T}(AA/A)\cdot\mathcal{T}(A/A)}\Big).$$

Using the standard Plünnecke inequality, that is if $|AA|$ or $|A/A|$ is $\le M|A|$, then $|AA/A| \le M^3|A|$ (see e.g. [45]) and the Szemerédi–Trotter Theorem 1.1 or Theorem 1.2, we arrive in the following corollary.

Corollary 4.2. *If $|AA| \le M|A|$ or $|A/A| \le M|A|$, then*

$$\mathsf{T}_3(A) \ll M^{12}|A|^4 \log |A|,$$

the same holds with $M = 1$ if A is replaced by Γ, a multiplicative subgroup in $\mathbb{F}_p^\times$ with $O(\sqrt{p})$ elements.

We remark that in the context of multiplicative subgroups Γ, when $|\Gamma| = O(\sqrt{p})$ the bound $\mathcal{T}(\Gamma) \ll |\Gamma|^4 \log |\Gamma|$ can be found in [35, Proposition 1].

Remark 4.3. Corollary 4.2 (in the case of small multiplicative subgroups) improves some results of the fourth author, see [40]. Upper bounds for $\mathsf{T}_3(\Gamma)$ have interesting applications to number-theoretic congruences studied, e.g. by Cilleruelo and Garaev [5], [6].

Consider the case when $\Gamma \subset (\mathbb{Z}/p^2\mathbb{Z})^*$, and $|\Gamma|$ divides $p-1$. One can consider the subgroup $\Gamma' \subseteq \mathbb{F}_p$ where $\Gamma' = \Gamma \pmod p$. It is easy to check that $|\Gamma'| = |\Gamma|$ and hence $\mathsf{T}_k(\Gamma) \le \mathsf{T}_k(\Gamma')$. Using this and the method of the proof of Lemma 4.1 and [35, Proposition 1], one can deduce the following statement.

Lemma 4.4. *Let Γ be subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ and let $|\Gamma| = t$. If $t \le p^{1/2}$ then $\mathsf{T}_3(\Gamma) \lesssim t^4$. If $t = p^{1/2+\delta}$, then $\mathsf{T}_3(\Gamma) \lesssim t^{4+6\delta}$.*

The reader can also find the previous bounds for $\mathsf{T}_3(\Gamma)$ in the paper [20], which were obtained purely by Stepanov's method. To avoid repeating the above-mentioned proofs, we content ourselves with merely a sketch of the proof of Lemma 4.4 further in this paper.

In the forthcoming proofs we avoid keeping track of exact powers of M and $\log |A|$ to make the formulae shorter; the reader is invited to check that they are indeed as presented in the statement of the theorem. The next lemma is crucial; its predecessor can be found in [33, Section 4].

Lemma 4.5. *Let* $1 \le \Delta \le |A|$ *and*

$$\mathsf{E}(A) = \mathsf{E}' + \mathsf{E}'' := \sum_{x: r_{A-A}(x) \le \Delta} r^2_{A-A}(x) \ + \sum_{x: r_{A-A}(x) > \Delta} r^2_{A-A}(x).$$

One has the inequality

$$\mathsf{E}'^6 \le |A|^6 \mathsf{E}_3(A) \Delta^2 \Sigma, \tag{4.3}$$

where

$$\Sigma := \sum_{d,d'} r_{A-A}(d) r_{A-A}(d') r^2_{A-A}(d-d'). \tag{4.4}$$

We are now ready to prove Theorem 1.4.

Proof. We use Lemma 4.5 with the choice of $\Delta \sim_M |A|^{11/20}$ (that is we omit the exact powers of M and $\log |A|$). Then we are done with the proof of Theorem 1.4 if $\mathsf{E}'' \gg \mathsf{E}(A)$, owing to estimate (2.7) of Lemma 2.1.

We proceed assuming that $\mathsf{E}' \gg \mathsf{E}(A)$. Denote $P := A - A$.

The quantity Σ in (4.4) counts solutions of the equation

$$a - a' = b - b' = (a_1 - a_2) - (a_3 - a_4), \tag{4.5}$$

with all the variables in A.

Let us introduce a cutoff parameter $\tau \sim_M |A|^{3/5}$ whose value is to be justified shortly. We now partition $P = P' \cup P''$ the set $A - A$ into the set of "poor" and "rich" elements, namely

$$P' = \{d : \ r_{A-A}(d) \le \tau\}, \qquad P'' = P \setminus P'.$$

Correspondingly,

$$\Sigma = \Sigma' + \Sigma'',$$

where Σ' is the restriction of the count (4.5) to the case when $(d = a - a' = b - b') \in P'$.

Clearly,

$$\begin{aligned} \Sigma' &\le \tau |\{a_1 - a_2 = (a_3 - a_4) - (a_5 - a_6) : \ a_1, \dots, a_6 \in A\}| = \tau \mathsf{T}_3(A) \\ &\le_M \tau \mathcal{T}(A) \qquad (4.6) \\ &\lesssim \tau |A|^4, \end{aligned}$$

by Lemma 4.1 and (4.2).

On the other hand, for $P'' = \{d : \ r_{A-A}(d) > \tau\}$, Lemma 2.1 provides a cardinality bound, decreasing as τ^{-3}. We need a slightly more elaboration, a dyadic partitioning to be soon summed as a vanishing geometric progression to show that as to P'', one can roughly assume that $r_{A-A}(d) \ll \tau$, for all $d \in P''$.

Namely, $j \ge 1$ set

$$P''_j := \{d : \ 2^{j-1}\tau \le r_{A-A}(d) < 2^j \tau\}.$$

Then, denoting for simplicity $2^j\tau = \tau_j$, one has, by (2.6),

$$|P_j''| \ll \frac{M^2|A|^3}{\tau_j^3}. \tag{4.7}$$

Setting Σ_j'' to be the corresponding to P_j'' component of Σ'', that is when the sum in (4.4) is restricted to $d - d' \in P_j''$, we can bound

$$\begin{aligned}\Sigma_j'' &\le \tau_j^2|\{(d,a_1,a_2,a_3,a_4) \in P_j'' \times A \times \dots \times A) :\ d = (a_1-a_2)-(a_3-a_4)\}| \\ &\le \tau_j^2\sqrt{\mathsf{E}(A,P_j'')}\sqrt{\mathsf{T}_3(A)},\end{aligned}$$

by Cauchy–Schwarz.

We substitute (4.7) to claim, by (2.4), Lemma 2.1:

$$\mathsf{E}(P_j'',A) \ll M|A||P_j|^{3/2} \ll_M |A|^{11/2}\tau_j^{-9/2}.$$

Furthermore, $\mathsf{T}_3(A) \lesssim_M |A|^4$ as above, by Lemma 4.1 and (4.2).

Thus

$$\Sigma'' \lesssim_M \tau^{-1/4}|A|^{19/4}\sum_{j\ge 1} 2^{-j/4} \ll \tau^{-1/4}|A|^{19/4}.$$

We now match the latter estimate and (4.6) for Σ': this prompts the choice $\tau \sim_M |A|^{3/5}$ (that is up to powers of M and $\log|A|$) and proves that

$$\Sigma \lesssim_M |A|^{23/5}. \tag{4.8}$$

We now go back to the main estimate (4.3) of Lemma 4.5. We have, by Lemma 2.1, the fact that $\mathsf{E}_3(A) \lesssim_M |A|^3$ and the assumption $\mathsf{E}(A) \gg \mathsf{E}'$ in the statement of Lemma 4.5 ends the proof of Theorem 1.4 after substituting $\Delta = |A|^{11/20}$ in the lemma's estimate. Indeed, we get

$$\mathsf{E}^6(A) \lesssim_M |A|^6 \cdot |A|^3 \cdot |A|^{11/10} \cdot |A|^{23/5} = |A|^{147/10}. \qquad \square$$

5. Proofs of main lemmata

5.1. Proof of Lemma 4.1.

Proof. Clearly, for any triple $(h_1,h_2,h_3) \in A \times A \times A$ and $a \in A$ we have

$$\begin{aligned}h_1 - h_2 - h_3 &= (h_1-h_2)\left(1-\frac{h_3}{h_1}\right) - \frac{h_2h_3}{h_1} \\ &= (ah_1 - ah_2)\left(a^{-1} - a^{-1}\frac{h_3}{h_1}\right) - \frac{h_2h_3}{h_1}.\end{aligned}$$

Set $\alpha = a^{-1}\frac{h_3}{h_1} \in A/AA$, $\beta = ah_2 \in AA$. Then we have the following estimate, where the first line follows from the latter identity, and in the

second line the Cauchy–Schwarz inequality and interchange of the order of summation have been applied:

$$\begin{aligned}\mathsf{T}_3(A) &= \sum_x r^2_{A-2A}(x)\\ &\leqslant |A|^{-2}\sum_x \left(\sum_{\alpha\in A/AA,\,\beta\in AA} r_{(A^{-1}-\alpha)(AA-\beta)}(x+\alpha\beta)\right)^2\\ &\leqslant \frac{|AA||A/AA|}{|A|^2}\sum_{\alpha\in A/AA,\,\beta\in AA}\sum_x r^2_{(A^{-1}-\alpha)(AA-\beta)}(x)\,.\end{aligned}$$

The three-index sum in the right-hand side is the number of solutions of the equation

$$(b-\alpha)(c-\beta)=(b'-\alpha)(c'-\beta):\ \alpha\in A/AA,\ \beta\in AA,\ b,b'\in A^{-1},\ c,c'\in AA,$$

or, after rearranging, of the equation (with the same variables)

$$\frac{b-\alpha}{b'-\alpha}=\frac{c'-\beta}{c-\beta}. \tag{5.1}$$

The left-hand side of the latter equation, since $A^{-1}\subseteq A/AA$, has all its variables $b,b',\alpha\in A/AA$, the right-hand side $c,c',\beta\in AA$. Applying once again the Cauchy–Schwarz inequality, the number of solutions of the latter equation is bounded by $\sqrt{\mathcal{T}(A/AA)\cdot\mathcal{T}(AA)}$.

This completes the proof, once we note that $|AA/A|=|A/AA|$ and that one could implement the above procedure for any $a\in A^{-1}$, rather than $a\in A$. □

5.2. Sketch of Proof of Lemma 4.4. According to Lemma 4.1 we need to find upper bound for the number of solution to the equation

$$(a-b)(a'-c')=(a-c)(a'-b'):\ a,b,c,a',b',c'\in\Gamma'\equiv\Gamma \pmod p.$$

Here we follow the scheme of the proof of Proposition 1 of the paper [35]. It is easy to see that for any tuple (a,b,c,a',b',c') satisfying the above equation, the points $(a,a'),(b,b'),(c,c')$ lie on the same line and one can assume that these points are pairwise distinct. One can restrict the set of lines to only those in the form

$$ux+vy=1.$$

Define $l_{u,v}=|\{(x,y)\in\Gamma'\times\Gamma' : ux+vy=1\}|$. So, we need to get an upper estimate for the sum

$$\sum_{u,v} l^3_{u,v}\,.$$

Such an estimate follows from Theorem 1.2 after easy calculations. For the case of $|\Gamma|=O(\sqrt{p})$ this method gives a near-optimal estimate, when

$\delta \neq 0$, the claim of Lemma 4.4 follows by application of the Hölder inequality.

5.3. Proof of Lemma 4.5. The proof represents an instance of the eigenvalue method developed by the third author.

Proof. Consider a $|A| \times |A|$ matrix $\mathfrak{M}$, with elements $\mathfrak{M}_{ab} = \sqrt{r_{A-A}(a-b)}$. In addition, let $\mathfrak{R}$ be the matrix with entries $\mathfrak{R}_{ab} = r_{A-A}(a-b)$.

We observe that both matrices have positive entries, are symmetric, and the matrix $\mathfrak{R}$ is semipositive-definite. Indeed, for any vector $\boldsymbol{v} \in \mathbb{R}^{|A|}$, identifying A with its characteristic function, the same for its shifts, say $A + (a-b)$ below, we have, after a rearrangement

$$\begin{aligned}\boldsymbol{v} \cdot \mathfrak{R}\boldsymbol{v} &= \sum_{a,b,c} A(c)[A+(a-b)](c)v_a v_b \\ &= \sum_{a,b,c} [A-b](c-a)[A-a](c-a)v_a v_b \\ &= \sum_x \left(\sum_a [A-a](x)v_a \right)^2 .\end{aligned}$$

Let us calculate the trace $\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R})$ in two different bases. In the standard basis

$$\begin{aligned}(5.2)\quad &\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R}) \\ &= \sum_{x,y,z\in A} \sqrt{r_{A-A}(x-y)}\sqrt{r_{A-A}(y-z)}r_{A-A}(x-z) \\ &= \sum_{d,d'} \sqrt{r_{A-A}(d)}\sqrt{r_{A-A}(d')}r_{A-A}(d-d')|A\cap(A+d)\cap(A+d')| \\ &\le \left(\sum_{d,d'} |A\cap(A+d)\cap(A+d')|^2 \right)^{1/2} \\ &\qquad\qquad \times \left(\sum_{d,d'} r_{A-A}(d)r_{A-A}(d')r_{A-A}^2(d-d') \right)^{1/2} \\ &= \sqrt{\mathsf{E}_3(A)\Sigma}.\end{aligned}$$

Modulo a power of $|A|$ this gives the square root of the right-hand side in the lemma's estimate.

Let us now estimate $\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R})$ from below. Since both matrices have positive entries, the trace will not increase if we zero the elements $\mathfrak{M}_{ab}$, with $r_{A-A}(a-b) > \Delta$.

Let us now define the matrix $\mathfrak{M}'$ (see the forthcoming Remark 5.1 as to why) as follows:

$$\mathfrak{M}'_{ab} = \begin{cases} \Delta^{-1/2}\mathfrak{R}_{ab}, & \text{if } r_{A-A}(a-b) \le \Delta, \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

The matrix $\mathfrak{M}'$ is clearly symmetric, and we have an entry-wise bound $\mathfrak{M}'_{ab} \le \mathfrak{M}_{ab}$ for all $a, b \in A$.

We now get a lower bound on $\mathfrak{tr}(\mathfrak{M}'^2\mathfrak{R})$.

Consider the orthonormal basis $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_{|A|}\}$ of real eigenvectors of $\mathfrak{M}'$, the corresponding real eigenvalues being $\mu_1, \dots \mu_{|A|}$, ordered by non-increasing moduli. The eigenvector $\boldsymbol{v}_1$, corresponding to the principal eigenvalue μ_1 is non-negative by the Perron–Frobenius theorem.

Hence, since $\mathfrak{R}$ is semipositive-definite

$$\mathfrak{tr}(\mathfrak{M}'^2\mathfrak{R}) = \sum_{a\in A} \mu_a^2(\mathfrak{R}\boldsymbol{v}_a \cdot \boldsymbol{v}_a) \ge \mu_1^2(\mathfrak{R}\boldsymbol{v}_1 \cdot \boldsymbol{v}_1).$$

Since μ_1 is the spectral radius of $\mathfrak{M}'$, we have, with $\boldsymbol{v} = \frac{1}{\sqrt{|A|}}(1, \dots, 1)$,

$$\mu_1 = \boldsymbol{v}_1 \cdot \mathfrak{M}'\boldsymbol{v}_1 \ge \boldsymbol{v} \cdot \mathfrak{M}'\boldsymbol{v} = \Delta^{-1/2}\frac{\mathsf{E}'}{|A|}.$$

Furthermore, by non-negativity of $\mathfrak{R}$ and $\boldsymbol{v}_1$ and the previous estimate,

$$\boldsymbol{v}_1 \cdot \mathfrak{R}\boldsymbol{v}_1 \ge \Delta^{1/2}\boldsymbol{v}_1 \cdot \mathfrak{M}'\boldsymbol{v}_1 \ge \frac{\mathsf{E}'}{|A|}.$$

This completes the proof of Lemma 4.5. □

Remark 5.1. In the case of a multiplicative subgroup Γ, the proof could be made slightly more straightforward, for the reason from passing from $\mathfrak{M}$ to $\mathfrak{M}'$ in (5.3) was that otherwise we would need additional argument as to how $\mathfrak{R}\boldsymbol{v}_1 \cdot \boldsymbol{v}_1$, where $\boldsymbol{v}_1$ is the principal eigenvector of $\mathfrak{M}$, compares to $\mathfrak{R}\boldsymbol{v} \cdot \boldsymbol{v}$, with $\boldsymbol{v} = \frac{1}{\sqrt{|A|}}(1, \dots, 1)$. In the multiplicative subgroup case $\boldsymbol{v} = \boldsymbol{v}_1$, for both matrices $\mathfrak{M}$ and $\mathfrak{R}$ are regular (in fact, circulant). This implies the lower bound

$$\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R}) \ge |A|^{-3}\mathsf{E}^2_{3/2}(A)\mathsf{E}(A),$$

where the notation $\mathsf{E}_{3/2}(A)$ was defined by (2.1). The latter estimate suffices to yield Theorem 1.4, for by the Hölder inequality

$$\mathsf{E}(A) \le \mathsf{E}_3(A)\mathsf{E}^{2/3}_{3/2}(A).$$

Previously best known energy bounds that Theorem 1.4 improves on, have been used in many papers, quoted in the introduction and beyond. The new bound (1.7) automatically results in improvement of estimates, which relied on its predecessors. This concerns, in particular, the results in [39], dealing with multiplicative energy of sumsets.

6. Additive energy of multiplicative subgroups

Studying translation properties of multiplicative subgroups in $\mathbb{F}_p^\times$ is a classical subject of number theory see, e.g., [16], [29]. In [12], [13] it was proved, in particular, that $\mathsf{E}(\Gamma) \ll |\Gamma|^{5/2}$ for any subgroup $\Gamma \subset \mathbb{F}_p$, with $|\Gamma| \le p^{2/3}$. It is well known that the latter bound is optimal for subgroups of size $\Omega(p^{2/3})$. In [32] better energy bounds for multiplicative subgroups of smaller size were obtained. Theorem 1.4 sets the new record for $|\Gamma| = O(p^{1/2})$. It also allows for some improvement of the "intermediate range" bounds for $\Omega(p^{1/2}) = |\Gamma| = O(p^{2/3})$, presented in this section.

Let us restate the results that we are going to use. See the beginning of Section 4 for some of the notation used.

Corollary 6.1. *Let $\Gamma \subseteq \mathbb{F}_p^\times$ be a multiplicative subgroup, $|\Gamma| \leqslant \sqrt{p}$. Then*

$$\mathsf{T}_3(\Gamma) \le \mathcal{T}(\Gamma) \ll |\Gamma|^4 \log |\Gamma| \,, \tag{6.1}$$

and

$$\mathsf{E}(\Gamma) \ll |\Gamma|^{49/20} \log^{1/5} |\Gamma| \,. \tag{6.2}$$

To get new energy bounds for intermediate size subgroups, we apply the standard technique from the literature cited below and the following theorem [19, Theorem 1.2] which replaces the bound (6.1).

Theorem 6.2. *Let $\Gamma \subset \mathbb{F}_p^\times$ be an arbitrary multiplicative subgroup. Then*

$$\mathcal{T}(\Gamma) - \frac{|\Gamma|^6}{p} \ll \begin{cases} p^{1/2}|\Gamma|^{7/2}, & \text{if } |\Gamma| \geqslant p^{2/3}, \\ |\Gamma|^5 p^{-1/2}, & \text{if } p^{2/3} > |\Gamma| \geqslant p^{1/2}\log p, \\ |\Gamma|^4 \log |\Gamma|, & \text{if } |\Gamma| < p^{1/2}\log p. \end{cases}$$

Remark 6.3. Using Theorem 6.2 one can sightly improve the upper bound for $\mathsf{T}_3(\Gamma)$, $\Gamma \subseteq \mathbb{Z}/p^2\mathbb{Z}$ in Lemma 4.4; we leave this to a keen reader.

The changes to estimate (6.2) we are about to address are also due to the fact that the estimates of Theorem 6.2 have replaced (6.1), and besides that the full analogue of the second inequality in (2.5) from Lemma 2.1 (used once in the proof of (6.2)) for subgroups $|\Gamma| \leqslant p^{2/3}$ is as follows.

Lemma 6.4. *Let $\Gamma \subset \mathbb{F}_p^\times$ be a multiplicative subgroup, $|\Gamma| \leqslant p^{2/3}$. Then and for any Γ–invariant set $Q \subset \mathbb{F}_p^\times$ (i.e. $Q\Gamma = Q$) one has*

$$\mathsf{E}(Q,\Gamma) \ll \frac{|\Gamma|^2|Q|^2}{p} + |\Gamma||Q|^{3/2} \,. \tag{6.3}$$

Namely for $|\Gamma| = \Omega(p^{1/2})$, one has to add to the second estimate in 2.5 the "statistical average", see, e.g., [30] or [32]. Note that the format of second term in (6.3) complies with using the point-plane theorem of [26], see also [25].

We now present the new energy bound, improving the bound $\mathsf{E}(\Gamma) \ll |\Gamma|^{5/2}$ (sharp for $|\Gamma| \sim p^{2/3}$) for subgroups with $|\Gamma| \lesssim p^{5/8}$.

Theorem 6.5. *Let $\Gamma \subseteq \mathbb{F}_p^\times$ be a multiplicative subgroup, with $p^{1/2} \leqslant |\Gamma| \leqslant p^{2/3}$. Then*

$$\mathsf{E}(\Gamma) \ll \log^{1/4}|\Gamma| \cdot \max\left\{ \left(\frac{|\Gamma|^{104}}{p^3}\right)^{1/40}, \left(\frac{|\Gamma|^{68}}{p^5}\right)^{1/24} \right\}. \tag{6.4}$$

Outline of the proof. Set $L = \log|\Gamma|$. We repeat the arguments of the proof of Theorem 1.4, estimating $\mathcal{T}(\Gamma)$ as $\mathcal{T}(\Gamma) \ll L|\Gamma|^6/p$, according to Theorem 6.2. To bound energies $\mathsf{E}(P_j'', \Gamma)$ which appear in the proof, see estimate (4.7) and argument following it, we use the estimate (6.3) of Lemma 6.4. If the second term in the application of (6.3) dominates, we literally repeat the proof of Theorem 1.4, obtaining

$$\mathsf{E}(\Gamma) \ll \log^{1/5}|\Gamma| \cdot \left(\frac{|\Gamma|^{104}}{p^3}\right)^{1/40}.$$

Observe that owing to Remark 2.2 the estimates of Lemma 2.1 on $\mathsf{E}_3(\Gamma)$, as well (4.7) remain valid.

It is easy to see that apart from the above estimate on $\mathcal{T}(\Gamma)$, the alternative case of the estimate of Lemma 6.4 is the only modification to the proof of Theorem 1.4 required. A straightforward calculation leads to choosing in the later case the value of the parameter τ in the proof of Theorem 1.4 as $\tau = |\Gamma|^{5/3}p^{-2/3}$, which then yields the inequality

$$\mathsf{E}^4_{3/2}(\Gamma)\mathsf{E}^2(\Gamma) \ll L|\Gamma|^9\mathcal{T}(\Gamma)\cdot\tau \ll L^2|\Gamma|^9\frac{|\Gamma|^6}{p}\cdot\tau\,.$$

Substituting $\tau = |\Gamma|^{5/3}p^{-2/3}$ and using the Hölder inequality to get rid of $\mathsf{E}^4_{3/2}(\Gamma)$, see Remark 5.1, we have

$$\mathsf{E}^6(\Gamma) \ll L^2|\Gamma|^{15}p^{-1}(|\Gamma|^{5/3}/p^{2/3})\cdot(|\Gamma|^3/\mathsf{E}(\Gamma))^2\,.$$

and therefore

$$\mathsf{E}(\Gamma) \ll L^{1/4}\cdot\left(\frac{|\Gamma|^{68}}{p^5}\right)^{1/24}. \qquad \square$$

Bound (6.4) is better than the previously best known one in [32, Theorem 8] for subgroups of size $p^{1/2} \leqslant |\Gamma| \lesssim p^{4/7}$.

It was proved in [34] that for any multiplicative subgroup such that $|\Gamma| \gg p^{1/2}\log^{1/3} p$, and $-1 \in \Gamma$ one has $\mathbb{F}_p^* \subseteq 5\Gamma$. We finish this section adding one more result about basis properties of subgroups and show, in particular, that the restriction $-1 \in \Gamma$ can be omitted.

Corollary 6.6. *Let $\Gamma \subseteq \mathbb{F}_p^\times$ be a multiplicative subgroup. Then for all sufficiently large p if $|\Gamma| \geqslant \sqrt{p}\log p$, then $|3\Gamma| > p/2$. In particular, $\mathbb{F}_p^* \subseteq 5\Gamma$.*

Proof. Using the second part of Theorem 6.2, combining with Lemma 4.1, we obtain

$$\sum_x \left(r_{\Gamma+\Gamma+\Gamma}(x) - \frac{|\Gamma|^3}{p}\right)^2 \ll |\Gamma|^5 p^{-1/2}\,. \tag{6.5}$$

Hence if the complement to 3Γ is at least $p/2$, then we have

$$p/2 \cdot \frac{|\Gamma|^6}{p^2} \ll |\Gamma|^5 p^{-1/2}$$

and this is a contradiction for sufficiently large p.

To prove that $\mathbb{F}_p^* \subseteq 5\Gamma$ it is sufficiently to show that for any nonzero ξ the following holds $3\Gamma \cap (\xi\cdot\Gamma - 2\Gamma) \neq \emptyset$. But the last is trivial because the arguments above work for any sets of the form $\alpha\cdot\Gamma + \beta\cdot\Gamma + \gamma\cdot\Gamma$, where $\alpha,\beta,\gamma \neq 0$. □

6.1. On the greatest distance between the adjacent elements of cosets of a subgroup. Following Bourgain, Konyagin and Shparlinski [3], we introduce, for a multiplicative subgroup $\Gamma \subseteq \mathbb{F}_p^\times$ of order t, the maximum gap $H_p(t)$ between elements of cosets of Γ, as follows:

$$H_p(t) = \max\{H : \exists\, a \in \mathbb{F}_p^*, \exists\, u \in \mathbb{F}_p, 1 \leq j \leq H : u + j \in \mathbb{F}_p \setminus a\Gamma\}.$$

In [3, Theorem 3] the following bound was established.

Theorem 6.7. *For $t \geq p^{1/2}$, one has*

$$H_p(t) \leq p^{463/504+o(1)},\ p \to \infty.$$

The case $t \geq p^{1/2}$ is important, because for any $g > 1$ and for almost all p the subgroup generated by powers of g has cardinality at least $p^{1/2}$, see [24]. The distribution of the elements of this subgroup is closely related to the distribution of digits of $1/p$ in base g.

We use the symbol $o(1)$ in this section to subsume terms which are smaller than any power of p, most of these terms come from the forthcoming quote of [3, Theorem 1] as Theorem 6.10 here, to be used as a black box.

The above exponent $\frac{463}{504}$ was improved to $\frac{5977}{6552}$ in [40]. New estimates for additive energy of multiplicative subgroups allow for further improvement, as follows.

Theorem 6.8. *For $t \ge p^{1/2}$, one has*

$$H_p(t) \le p^{\frac{437}{480}+o(1)},\ p \to \infty.$$

Before proving Theorem 6.8, let us introduce several auxiliary quantities. Let g be the primitive root of $\mathbb{F}_p^\times$. $\Gamma \subseteq \mathbb{F}_p^\times$, as we said, is a multiplicative subgroup of order t; set $n = (p-1)/t$. Also let $\Gamma_j := g^j\Gamma$ and

$$S_j(t) := S(g^j, \Gamma) = \sum_{x\in\Gamma} e_p(g^j x); \qquad N_{j,t}(h) := |\{1 \le |u| \le h : u \in \Gamma_j\}|,$$

where e_p is the canonical additive character.

The quantities $H_p(t), N_{j,t}(h)$ and $S_j(t)$ are related via following statement [16, Lemma 7.1].

Theorem 6.9. *Iffor some $h \ge 1$ the inequality :*

$$\sum_{1\le j\le n} N_{j,t}(h)|S_{j+k}(t)| \le 0.5t$$

holds for all $k = 1, \dots, n$, then for any $\varepsilon > 0$

$$H_p(t) \ll p^{1+\varepsilon}h^{-1}.$$

Besides, it is easy to see that the quantity

$$N(\Gamma, h) := \sum_{1\le j\le n} N_{j,t}^2(h)$$

is the number of solutions to the congruence

$$ux \equiv y \pmod p, \qquad 0 < |x|, |y| \le h, u \in \Gamma\,.$$

In [3, Theorem 1], an upper bound for $N(\Gamma, h)$ was proved in the following form.

Theorem 6.10. *Let $\nu \ge 1$ be a fixed integer and let $t \gg p^{1/2}$, $p \to \infty$. Then*

$$N(\Gamma, h) \le ht^{\frac{2\nu+1}{2\nu(\nu+1)}}p^{\frac{-1}{2(\nu+1)}+o(1)} + h^2t^{1/\nu}p^{-1/\nu+o(1)}.$$

By orthogonality, it follows from definition of the quantity $S_j(t)$ that

$$\sum_{1\le j\le n} |S_j(t)|^4 < \frac{p}{t}\mathsf{E}(\Gamma). \tag{6.6}$$

We are now ready to prove Theorem 6.8.

Proof. The structure of the proof repeats its predecessors in [3] or [40]. Just as above $t := |\Gamma|$. By the Hölder inequality we obtain

$$\sum_{1\le j\le n} N_{j,t}(h)|S_{j+k}(t)| \le \left(\sum_{1\le j\le n} N_{j,t}(h)\right)^{1/2}\left(\sum_{1\le j\le n} N_{j,t}(h)^2\right)^{1/4}\left(\sum_{1\le j\le n} |S_j(t)|^4\right)^{1/4}.$$

For the three terms in the right–hand side we have estimates

$$\sum_{1\le j\le n} N_{j,t}(h) = 2h,$$
$$\sum_{1\le j\le n} N_{j,t}(h)^2 = N(\Gamma,h),$$

and (6.6).

Define $h = p^{43/480-\varepsilon}$ for some small fixed $\varepsilon > 0$.

Consider the case $t \in [p^{1/2}, p^{4/7}]$. Then by (6.4) one has

$$\mathsf{E}(\Gamma) \lesssim \left(\frac{|\Gamma|^{104}}{p^3}\right)^{1/40}.$$

We take $\nu = 6$ in the estimate of Theorem 6.10 for $N(\Gamma,h)$, in which case the second term in the estimate dominates. One can easily check that for such choice of parameters, the quantity

$$\sum_{1\le j\le n} N_{j,t}(h)|S_{j+k}(t)| \tag{6.7}$$

is less than $0.5t$.

Now consider the case when $t > p^{4/7}$. Then we merely write

$$\sum_{1\le j\le n} N_{j,t}(h)|S_{j+k}(t)| \le \max_j |S_j(t)| \sum_{1\le j\le n} N_{j,t}(h) \le p^{1/6+o(1)}t^{1/2}h.$$

The last inequality took advantage of the supremum estimate for $|S_j(t)|$ that we take from [34, Theorem 1]. It is easy to verify that the inequality

$$\sum_{1\le j\le n} N_{j,t}(h)|S_{j+k}(t)| \le 0.5t \tag{6.8}$$

also holds. With that, and taking sufficiently small $\varepsilon > 0$, the proof of Theorem 6.8 is completed. □

7. Sum set inequalities

We start out with a remark that one can repeat the proof of Theorem 1.4 with the matrix $\mathfrak{M}$ being replaced by the matrix of zeroes and ones, with $\mathfrak{M}_{ab}=1$ if the sum $a+b$ is popular, that is $r_{A+A}(a+b)\ge \frac{|A|^2}{2|A+A|}$.

This will not alter the structure of the proof, owing the identity

$$(b+a)-(c+a)=b-c, \quad \text{replacing} \quad (b-a)-(c-a)=b-c,$$

as well as the fact that the quantity $\mathsf{E}^+(A):=\sum_s r^3_{A+A}(s)$ satisfies the same upper bound as $\mathsf{E}_3(A)$ in (2.4), Lemma 2.1 — it would replace $\mathsf{E}_3(A)$ in the analogue of estimate (5.2).

After that the acme of getting the upper bound on $\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R})$ would remain to be estimate (4.8). However, estimating $\mathfrak{tr}(\mathfrak{M}^2\mathfrak{R})$ from below does present some challenge in the real case, owing to Remark 5.1. However, in the multiplicative subgroup case the matrices $\mathfrak{M}$, $\mathfrak{R}$ still have the same principal eigenvector if al ones, and one arrives in the following estimate: for $|\Gamma|\le\sqrt{p}$,

$$|\Gamma+\Gamma|\gg |\Gamma|^{8/5}\log^{-2/5}|\Gamma|.$$

The same estimate, with a slightly worse power of $\log|\Gamma|$ was established in [32]. We do not know how to improve the exponent $8/5$ for the sum set towards $7/3$ as we have for the difference set but would like to point out that both the sum set and the energy FPMS exponents have been now made dependent on the same estimate (4.8).

To circumnavigate the difficulty arising from the fact that principal eigenvectors of the matrices with elements $r_{A+A}(a+b)$ and $r_{A-A}(a-b)$ may be different for $M>1$, we present a different proof, resulting in a new FPMS-type sum-product inequality, with a "reasonable" M-dependence. Heuristically speaking, the better the FPMS-exponent, the weaker the inequality, treated as the usual sum-product inequality, namely when $|AA|\sim|A+A|$, cf. (1.5). In this sense, the following inequality (7.1) is slightly weaker than the classical Elekes one (1.4) and represents, in some sense a sum set analogue of (1.5).

We remark that on can find "middle-ground", that is non-trivial from the FPMS point of view (that is giving a FPMS exponent greater than $3/2$) and still stronger than (1.4), due, e.g., to Li and Roche-Newton [18] or the one used by Konyagin and Shkredov [15, Theorem 12] to derive their new sum-product bound. But as the FPMS aspect improves, the other aspect eventually becomes weaker than (1.4), the only exception (up to a log factor) being (1.6).

Theorem 7.1. *For a real set A one has the estimates*

$$|A+A|^{10}|AA|^{17}\gtrsim |A|^{33}. \tag{7.1}$$

The forthcoming proof of Theorem 7.1 uses the construction from [36, Proof of Theorem 10], which dealt with differences and led to (1.5). Its adaptation to sums rests on the following Lemma 7.2 — a stronger version of the argument from [27, Proof of Proposition 16] and [15, Section 4].

Proof. Denote $D = D(A) = A - A$, $S = S(A) = A + A$. Let $P \subseteq D$ be a popular energy subset of D by energy. Note that P, Δ throughout the paper have different meaning, and in this section these are not the quantities used in the proofs of Theorems 1.3 and 1.4, also different from one another. Namely, now P is defined as follows. There exists some $\Delta : \frac{\mathsf{E}(A)}{2|A|^2} \le \Delta \le |A|$, such that each $x \in P$ has approximately Δ, that is between Δ and 2Δ realisations and

$$\mathsf{E}(A) \sim \sum_{x\in P} r^2_{A-A}(x) \gtrsim |P|\Delta^2. \tag{7.2}$$

Such P exists by the dyadic version of the pigeonhole principle. We will not keep track of powers of $\log|A|$, for they go slightly out of hand in the proof of Lemma 7.2.

Furthermore, define a plane point set

$$\mathcal{P}(A) \subseteq A \times A := \{(a, a') :\ a - a' \in P\},\ \text{so}\ \ |\mathcal{P}(A)| \approx |P|\Delta. \tag{7.3}$$

Lemma 7.2. *There exists $\widetilde{A} \subseteq A$, with $|\widetilde{A}| \gg |A|$, a pair of subsets $A', A'' \subseteq \widetilde{A}$ and a natural number q with the following property: $|A'| \gtrsim |A''| \ge q$, $|A'| \gtrsim |A|$, and for each $a \in A'$ there are at least $q \sim |\mathcal{P}(\widetilde{A})|/|A|$ points $(a', a'') \in \mathcal{P}(\widetilde{A}) \cap (A' \times A'')$, where the point set $P(\widetilde{A}) \subseteq \widetilde{A} \times \widetilde{A}$ is the popular energy set defined in terms of $\widetilde{A}$ via* (7.2), (7.3).

Besides, $\mathsf{E}(\widetilde{A}) \sim \mathsf{E}(A', A'')$.

Informally, Lemma 7.2 claims that there exists a positive proportion (in fact, of density arbitrarily close to 1 as the proof shows) proportion subset $\widetilde{A}$ of A, such that much of the energy of $\widetilde{A}$ (up to factors of powers of $\log|A|$) is supported on some "regular" point set $\mathcal{P}'$, such that $\mathcal{P}'$ gets covered by a *wide* rectangle: $\mathcal{P}' \subseteq A' \times A'' \subseteq \widetilde{A} \times \widetilde{A}$, with, most importantly, the lower bound $|A'| \gtrsim |A|$, *and* (up to factors of powers of $\log|A|$) an expected lower bound of the number of points of $\mathcal{P}'$ for every abscissa $a' \in A'$. The lower bound $|A'| \gtrsim |A|$ strengthens the above-mentioned earlier statement in [27] and is crucial for the forthcoming argument.

We remark that the claim or Lemma 7.2 remains true for any finite ≥ 1 moment of the number-of-realisations function r_{A-A}, as well as its multiplicative analogue $r_{A/A}$.

We prove the lemma afterwards and now proceed with the proof of Theorem 7.1. Apply Lemma 7.2 and to ease on notation reset $\widetilde{A} = A$ and $\mathcal{P}(\widetilde{A}) = \mathcal{P}$. Let $\mathcal{P}' = \mathcal{P} \cap (A' \times A'')$.

For $\lambda \in A/A$ (nonzero, since $0 \notin A$) denote

$$A'_\lambda = \{a \in A : \lambda a \in A'\}, \ \text{ so } \ \lambda A'_\lambda \subseteq A'.$$

Also denote, for brevity

$$\mathsf{E}^\times = \sum_\lambda |A'_\lambda|^2, \tag{7.4}$$

so $\mathsf{E}^\times$ is the multiplicative energy of A' and A. In the sequel sums in λ mean sums over A/A. Clearly,

$$\sum_\lambda |A_\lambda| = |A|^2, \qquad \sum_\lambda |A'_\lambda| = |A||A'|. \tag{7.5}$$

Whether either $|A/A| = M|A|$ or $|AA| = M|A|$, does not affect the argument, for M only comes from estimate (2.4) in Lemma 2.1 that we restate:

$$\mathsf{E}_3(A'') \lesssim M^2|A||A''|^2, \qquad \mathsf{E}_3(A'_\lambda) = \mathsf{E}_3(\lambda^{-1}A'_\lambda) \lesssim M^2|A||A'_\lambda|^2. \tag{7.6}$$

Let us estimate the number $\mathcal{T}_\Lambda$ of collinear point triples in $S \times S \subset \mathbb{R}^2$ such that the point triples are supported just on the lines with slopes in $\Lambda = A/A$. For the total number of collinear point triples $\mathcal{T}(S) \geq \mathcal{T}_\Lambda$ in $S \times S$ we have the unconditional upper bound, which is the standard implication of the Szemerédi–Trotter theorem:

$$\mathcal{T}_\Lambda \leq \mathcal{T}(S) \lesssim |S|^4. \tag{7.7}$$

To get a lower bound on $\mathcal{T}_\Lambda$ we consider a line $y = \lambda x + d$, where some $d \in P$, $\lambda \in \Lambda$ and estimate the minimum number of points of $S \times S$, supported on this line.

This means, we are looking at some $a, b, a', b' \in A$ such that

$$a + b - \lambda(a' + b') = d.$$

The latter equation is satisfied if one chooses $b = \lambda b'$, with any $b' \in A'_\lambda$: for any $a' \in A'_\lambda$ there are at least q choices of $a \in A''$, where the number q comes from Lemma 7.2.

Hence, define a point set $\mathcal{Q}_\lambda \subseteq S \times S$ as follows:

$$\mathcal{Q}_\lambda := \{(a' + b, a + \lambda b) : a \in A,\ a', b \in A'_\lambda, \text{ and } (a, \lambda a') \in \mathcal{P}'\}. \tag{7.8}$$

so for $(x, y) \in \mathcal{Q}_\lambda$ we have

$$y - \lambda x = a - \lambda a',$$

and since $\lambda a' \in A'$, for each pre-image $a' \in A'_\lambda$ there are at lest q values of $a \in A''$, by Lemma 7.2, such that $a - \lambda a' \in P$.

The point set $\mathcal{Q}_\lambda \subset \mathbb{R}^2$ (by construction, see (7.8)) is supported on at most $|P|$ parallel lines with the slope λ, making therefore $|\mathcal{Q}_\lambda|$ incidences with these lines. The number of collinear triples in the set $\mathcal{Q}_\lambda$ on these lines,

giving the lower bound for the quantity $\mathcal{T}_\lambda$ is at least the uniform case (in other words, we use the Hölder inequality):

$$\mathcal{T}_\lambda \geq |P|(|\mathcal{Q}_\lambda|/|P|)^3 = |\mathcal{Q}_\lambda|^3/|P|^2.$$

Comparing this with (7.7) we obtain

$$|S|^4|P|^2 \gtrsim \sum_{\lambda\in\Lambda} |\mathcal{Q}_\lambda|^3. \tag{7.9}$$

For a fixed λ, by (7.8) and Cauchy–Schwarz, one has

$$q|A'_\lambda|^2 \leq |\mathcal{Q}_\lambda|^{1/2}X^{1/2}, \tag{7.10}$$

where X is the number of solutions of the following system of equations:

$$a'+b=a''+b', \quad a+\lambda b=a'''+\lambda b' : \quad a',a'',b,b'\in A'_\lambda,\ a,a'''\in A''.$$

This can be rewritten as

$$\lambda(a'-a'')=\lambda(b'-b)=a-a'''.$$

For $d\in A-A$, let $r''(d), r'_\lambda(d)$ denote the number of realisations of d as a difference in $A''-A''$ and $A'_\lambda-A'_\lambda$, respectively. Then we have, tautologically by definition of X and then Hölder inequality

$$X \leq \sum_d r''(d)r'_\lambda(d)r'_\lambda(d) \leq \mathsf{E}_3^{1/3}(A'')\mathsf{E}_3^{2/3}(A'_\lambda),$$

We can now proceed with (7.10) by applying (7.6) to the above estimate for the quantity X, getting

$$q|A'_\lambda|^2 \leq |\mathcal{Q}_\lambda|^{1/2}(M^{1/3}|A|^{1/6}|A''|^{1/3})(M^{2/3}|A|^{1/3}|A'_\lambda|^{2/3}).$$

Before summing over $\lambda\in A/A$ let us rearrange as follows:

$$q|A''|^{-1/3}|A|^{-1/2}|A'_\lambda|^3 \leq M|\mathcal{Q}_\lambda|^{1/2}|A'_\lambda|^{5/3}, \tag{7.11}$$

We now sum in λ. In the right-hand side of (7.11) we apply the Hölder inequality:

$$\sum_\lambda |\mathcal{Q}_\lambda|^{1/2}|A'_\lambda|^{5/3} \leq \left(\sum_\lambda |\mathcal{Q}_\lambda|^3\right)^{1/6}\left(\sum_\lambda |A'_\lambda|^2\right)^{5/6}.$$

In the left-hand side of (7.11) use the Cauchy–Schwarz inequality and relations (7.4), (7.5):

$$\mathsf{E}^\times = \sum_\lambda |A'_\lambda|^{1/2}|A'_\lambda|^{3/2} \leq \sqrt{|A||A'|}\sqrt{\sum_\lambda |A'_\lambda|^3}.$$

Applying the standard Cauchy–Schwarz estimate $\mathsf{E}^\times \geq (|A||A|')^2/(M|A|)$ yields

$$\sum_\lambda |\mathcal{Q}_\lambda|^3 \geq M^{-6}|A|^{-9}q^6|A''|^{-2}|A'|^{-6}\mathsf{E}^{\times 7} \geq M^{-13}|A|^{-2}q^6|A''|^{-2}|A'|^8,$$

Thus by (7.9) one has

$$|S|^4 \gtrsim M^{-13}|A|^{-2}q^6|A''|^{-2}|A'|^8|P|^{-2}.$$

Using Lemma 7.2 we have the worst possible case $q^6|A''|^{-2}|A'|^8 \gtrsim (|P|\Delta)^6$, thus

$$|S|^4 \gtrsim M^{-13}|A|^{-2}|P|^4\Delta^6 \gtrsim M^{-13}|A|^{-2}\mathsf{E}^4(A)\Delta^{-2}.$$

The claim of Theorem 1.3 now follows from the upper bound

$$\Delta \le \mathsf{E}_3(A)/\mathsf{E}(A) \lesssim M^2|A|^3/\mathsf{E}(A),$$

where for $\mathsf{E}_3(A)$ we use (2.4), and the standard Cauchy–Schwarz lower bound $\mathsf{E}(A) \ge |A|^4/|S|$. □

7.1. Proof of Lemma 7.2.

Proof. The proof is a pigeonholing argument.

For brevity sake round up the values of all logarithms to integers. In the notation of the proof of Theorem 7.1 curtail $\mathcal{P} = \mathcal{P}(A)$. Partition A in at most $\log|A|$ nonempty sets by popularity of abscissae in $\mathcal{P}$. That is for $i = 1, \dots, \log|A|$ each abscissa from the set A_i supports between 2^{i-1} (inclusive) and 2^i (non-inclusive) points of $\mathcal{P}$. Let us set $q_i = 2^i$ and further in the proof use $\approx q_i$ as a shortcut for a number between 2^{i-1} and 2^i. For $i = 1, \dots, \log|A|$ take $\mathcal{P}_i$, defined as the set of all points of $\mathcal{P}$ with abscissae in A_i and dyadically partition the set of its ordinates by popularity as the union of sets A_i^j.

As a result, $\mathcal{P}$ is covered by the union of at most $\log^2|A|$ disjoint rectangles $A_i \times A_i^j$. By a *rectangle* we mean Cartesian product. By symmetry we can transpose i and j, so there is another cover symmetric with respect to the bisector $y = x$.

By the pigeonhole principle, at least one half of the mass $|\mathcal{P}| \approx |P|\Delta$ lies in "rich" rectangles A_i^j, each containing at least $\frac{1}{2\log^2|A|}|P|\Delta$ points of $\mathcal{P}$. Rather than writing out powers of 2 arising after such popularity arguments explicitly, we will often subsume them in the $\gg, \ll, \approx$ symbols.

There are two cases to consider.

Case 1. One of the rich rectangles has width or height, say $\gg |A|\log^{-10}|A|$. Then there is another, symmetric with respect to the $y = x$ bisector, and we are almost done, choosing the wider of the two rectangles.

Indeed, let $\mathcal{R}_i^j$ denote such a rich rectangle. We set A'' to be its projection on the y-axis.

Furthermore, $\mathcal{R}_i^j$ has base A_i, with $|A_i| \ge |A''|$ and $|A_i| \gg |A|\log^{-10}|A|$ (by how the case has been defined). For each $a \in A_i$ there are $\approx q_i$ points of $\mathcal{P}$. In particular, there are $\ll q_i$ points of $\mathcal{P} \cap \mathcal{R}_i^j$ with a given abscissa $a \in A_i$. Clearly, $|A_i|q_i \ll |P|\Delta$ (the total number of points in $\mathcal{P}$) thus the

maximum number of points of $\mathcal{P}$ in $\mathcal{R}_i^j$ with the same abscissa $a \in A_i$ is trivially

$$q_i \ll |P|\Delta/|A_i|. \tag{7.12}$$

On the other hand, $\mathcal{R}_i^j$ is rich, that is contains $\gg \frac{1}{\log^2|A|}|P|\Delta$ points of $\mathcal{P}$. We refine its base A_i to the set A' of rich abscissae, supporting at least $q := \frac{1}{16}\frac{1}{|A_i|}\frac{1}{\log^2|A|}|P|\Delta$ points of $P \cap \mathcal{R}_i^j$ each; by the pigeonhole principle these abscissae in A' still support $\gg \frac{1}{\log^2|A|}|P|\Delta$ points of $\mathcal{P} \cap \mathcal{R}_i^j$.

Clearly, $q \le |A''|$, the total number of ordinates in $\mathcal{R}_i^j$.

Since the maximum number of points of $\mathcal{P}$ per abscissa in A_i is q_i, the minimum number of the latter rich abscissae is

$$|A'| \gg \frac{1}{q_i}\frac{1}{\log^2|A|}|P|\Delta \gg \frac{1}{\log^2|A|}|A_i|,$$

by (7.12). Recall that by construction $|A_i| \ge |A''|$, as well as $|A_i| \gg |A|\log^{-10}|A|$, so $|A'| \gtrsim |A''|$ and $|A'| \gtrsim |A|$. Thus, but for the last claim of the lemma about energy, to be dealt with in the very end of the proof, we are done with Case 1, having found the sets A', A'' and $\widetilde{A} = A$.

Case 2. Let us show that Case 1 is the generic one, that is if there are no sufficiently wide or high rich rectangles apropos of $\mathcal{P}(A)$, we can refine A to its (arbitrarily) high proportion subset $\widetilde{A}$ and find ourselves in Case 1, relative to the point set $\mathcal{P}(\widetilde{A}) \subseteq \mathcal{P}(A)$.

Indeed, suppose there are no sufficiently wide or high rich rectangles A_i^j in the above constructed covering of $\mathcal{P}(A)$ by rectangles, that is both projections of each rich rectangle are $\le |A|\log^{-10}|A|$ in size. Then we remove from A the union $A_i \cup \bigcup_j A_i^j$, calling the resulting set A_1. By construction, crudely, $|A_1| \gg (1 - \log^{-5}|A|)|A|$.

On the other hand, at least half of the mass of $\mathcal{P}(A)$ has been removed. This means loss of at least a third of the energy. Indeed, $\mathcal{P}$ is supported on the union of $|\Delta|$ lines with the number of points of $A \times A$ on each line ranging between N and $2N$ and now at least half of the point set $\mathcal{P}$ has been deleted. Let us estimate from below the difference $\mathsf{E}(A) - \mathsf{E}(A_1)$.

To minimise the amount of energy lost after the deletion of half of the point set $\mathcal{P}(A)$, supported on P lines, each supporting between Δ and 2Δ of $A \times A$) one should be deleting the poorest lines, one by one (stopping in the midst of a line is also allowed). To this end, the extremal case arises if half of the mass of $\mathcal{P}$ were supported on lines with minimum occupancy Δ and the other half on lines with maximum occupancy 2Δ. In this extremal case one has $|\mathcal{P}| = 4|P|\Delta/3$, the total energy $2|P|\Delta^2$ being supported on $|P|$ lines. Deleting the $2|P|/3$ poorest lines means being left with two-thirds of the energy.

Thus $\mathsf{E}(A_1) \le (1 - \frac{1}{3}\log^{-1}|A|)\mathsf{E}(A)$.

So we pass from A to A_1 and check if we are in Case 1 apropos of $\mathcal{P}(A_1)$. If yes, we are done (modulo the coming claim about energy), otherwise we iterate the Case 2 deletion procedure. Once we have encountered Case 2, say $\log^5|A|$ times, we still retain a large subset, of A, containing a fraction of A, bounded from below as $\Omega((1-\log^{-5}|A|)^{\log^5|A|}) \gg 1$. The energy of this remaining large subset, however, is at most

$$\left(1 - \frac{1}{3}\log^{-1}|A|\right)^{\log^5|A|} \mathsf{E}(A) = o(|A|^2),$$

which is a contradiction. Thus at some point throughout iteration we must encounter Case 1.

To verify the final claim of the lemma about energy, it suffices to assume that the desired pair A', A'' has been found in Case 1 immediately, that is $\widetilde{A} = A$. Clearly,

$$\mathsf{E}(A', A'') \le \mathsf{E}(A) \sim |P|\Delta^2.$$

On the other hand, the rectangle $\mathcal{R} = A' \times A''$ still contains $\sim |P|\Delta$ points of P, which are all supported on at most $|P|$ lines.

Thus

$$\sum_{x \in P} r_{A'-A''}(x) \gg |P|\Delta.$$

It follows by Cauchy–Schwarz that

$$\mathsf{E}(A', A'') \gg \sum_{x \in P} r^2_{A'-A''}(x) \gg |P|\Delta^2 \sim \mathsf{E}(A). \qquad \square$$

References

[1] A. Balog & T. D. Wooley, "A low-energy decomposition theorem", *Q. J. Math* **68** (2017), p. 207-226.

[2] J. Bourgain & M.-C. Chang, "On the size of k-fold sum and product sets of integers", *J. Am. Math. Soc.* **17** (2004), no. 2, p. 473-497.

[3] J. Bourgain, S. V. Konyagin & I. E. Shparlinski, "Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm", *Int. Math. Res. Not.* **2008** (2008), article ID rnn090 (29 pages).

[4] M.-C. Chang & J. Solymosi, "Sum-product theorems and incidence geometry", *J. Eur. Math. Soc.* **9** (2007), no. 3, p. 545-560.

[5] J. Cilleruelo & M. Z. Garaev, "The congruence $x^x = \lambda \pmod p$", *Proc. Am. Math. Soc.* **144** (2016), no. 6, p. 2411-2418.

[6] ———, "Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications", *Math. Proc. Camb. Philos. Soc.* **160** (2016), no. 3, p. 477-494.

[7] G. Elekes, "On the number of sums and products", *Acta Arith.* **81** (1997), no. 4, p. 365-367.

[8] G. Elekes, M. B. Nathanson & I. Z. Ruzsa, "Convexity and sumsets", *J. Number Theory* **83** (2000), no. 2, p. 194-201.

[9] G. Elekes & I. Z. Ruzsa, "Few sums, many products", *Stud. Sci. Math. Hung.* **40** (2003), no. 3, p. 301-308.

[10] P. Erdős & E. Szemerédi, "On sums and products of integers", in *Studies in pure mathematics*, Birkhäuser, 1983, p. 213-218.

[11] A. Granville & J. Solymosi, "Sum-product formulae", in *Recent trends in combinatorics*, The IMA Volumes in Mathematics and its Applications, vol. 159, Springer, 2016, p. 419-451.
[12] D. R. Heath-Brown & S. V. Konyagin, "New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum", *Q. J. Math* **51** (2000), no. 2, p. 221-235.
[13] S. V. Konyagin, "Estimates for trigonometric sums and for Gaussian sums", in *IV International conference "Modern problems of number theory and its applications"*, 2002, p. 86-114.
[14] S. V. Konyagin & I. D. Shkredov, "On sum sets of sets, having small product sets", *Tr. Mat. Inst. Steklova* **290** (2015), p. 304-316.
[15] ———, "New results on sum-products in $\mathbb{R}$", *Proc. Steklov Inst. Math.* **294** (2016), no. 78, p. 87-98.
[16] S. V. Konyagin & I. E. Shparlinski, *Character sums with exponential functions*, Cambridge Tracts in Mathematics, vol. 136, Cambridge University Press, 1999.
[17] L. Li, "On a theorem of Schoen and Shkredov on sumsets of convex sets", `https://arxiv.org/abs/1108.4382`, 2011.
[18] L. Li & O. Roche-Newton, "Convexity and a sum-product type estimate", *Acta Arith.* **156** (2012), no. 3, p. 247-255.
[19] S. Macourt, I. D. Shkredov & I. E. Shparlinski, "Multiplicative energy of shifted sugroups and bounds on exponential sums with trinomials in finite fields", `https://arxiv.org/abs/1701.06192`, to appear in *Can. J. Math.*, 2017.
[20] Y. V. Malykhin, "Bounds for exponential sums over p^2", *J. Math. Sci., New York* **146** (2007), no. 2, p. 5686-5696.
[21] D. A. Mit'kin, "Estimation of the total number of total number of the rational points on a set of curves in a simple finite field", *Chebyshevskiĭ Sb.* **4** (2003), no. 4, p. 94-102.
[22] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev & I. D. Shkredov, "New results on sum-product type growth over fields", *Mathematika* **65** (2019), no. 3, p. 588-642.
[23] B. Murphy, O. Roche-Newton & I. D. Shkredov, "Variations on the sum-product problem II", *SIAM J. Discrete Math.* **31** (2017), no. 3, p. 1878-1894.
[24] F. Pappalardi, "On the order of finitely generated subgroups of $\mathbb{Q}^*(\mathrm{mod}\ p)$ and divisors of $p-1$", *J. Number Theory* **57** (1996), no. 2, p. 207-222.
[25] O. Roche-Newton, M. Rudnev & I. D. Shkredov, "New sum-product type estimates over finite fields", *Adv. Math.* **293** (2016), p. 589-605.
[26] M. Rudnev, "On the number of incidences between planes and points in three dimensions", *Combinatorica* **38** (2018), no. 1, p. 219-254.
[27] M. Rudnev, S. Stevens & I. D. Shkredov, "On The Energy Variant of the Sum-Product Conjecture", `https://arxiv.org/abs/1607.05053v5`, to appear in *Rev. Mat. Iberoam.*, 2017.
[28] T. Schoen & I. D. Shkredov, "On sumsets of convex sets", *Comb. Probab. Comput.* **20** (2011), no. 5, p. 793-798.
[29] ———, "Additive properties of multiplicative subgroups of $\mathbb{F}_p$", *Q. J. Math* **63** (2012), no. 3, p. 713-722.
[30] ———, "Higher moments of convolutions", *J. Number Theory* **133** (2013), no. 5, p. 1693-1737.
[31] I. D. Shkredov, "Some applications of W. Rudin's inequality to problems of combinatorial number theory", *Unif. Distrib. Theory* **6** (2011), no. 2, p. 95-116.
[32] ———, "Some new inequalities in additive combinatorics", *Mosc. J. Comb. Number Theory* **3** (2013), no. 3-4, p. 237-288.
[33] ———, "Some new results on higher energies", *Tr. Mosk. Mat. O.-va* **74** (2013), p. 35-73.
[34] ———, "On exponential sums over multiplicative subgroups of medium size", *Finite Fields Appl.* **30** (2014), p. 72-87.
[35] ———, "On tripling constant of multiplicative subgroups", *Integers* **16** (2016), article ID A75 (9 pages).
[36] ———, "Some remarks on sets with small quotient set", *Sb. Math.* **208** (2017), no. 12, p. 1854-1868.
[37] I. D. Shkredov, E. V. Solodkova & I. V. Vyugin, "On the additive energy of Heilbronn's subgroup", *Mat. Zametki* **101** (2017), no. 1, p. 43-57.

[38] I. D. Shkredov & I. V. Vyugin, "On additive shifts of multiplicative subgroups", *Mat. Sb.* **203** (2012), no. 6, p. 81-100.
[39] I. D. Shkredov & D. Zhelezov, "On additive bases of sets with small product set", 1606.02320v2, to appear in *Int. Math. Res. Not.*, 2016.
[40] Y. N. Shteĭnikov, "Estimates of trigonometric sums over subgroups and some of their applications", *Mathematical Notes* **98** (2015), no. 4, p. 667-684.
[41] J. Solymosi, "Bounding multiplicative energy by the sumset", *Adv. Math.* **222** (2009), no. 2, p. 402-408.
[42] J. Solymosi & G. Tardos, "On the number of k-rich transformations", in *Proceedings of the 23rd annual symposium on computational geometry, SCG'07*, ACM Press, 2007, p. 227-231.
[43] S. Stevens & F. d. Zeeuw, "An Improved Point-Line Incidence Bound Over Arbitrary Fields", https://arxiv.org/abs/1609.06284v4, 2016.
[44] E. Szemerédi & W. T. Trotter, "Extremal problems in discrete geometry", *Combinatorica* **3** (1983), p. 381-392.
[45] T. Tao & V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, 2006.

Brendan Murphy
Heilbronn Institute for Mathematical Research
School of Mathematics, University Walk
Bristol BS8 1TW, UK
E-mail: brendan.murphy@bristol.ac.uk

Misha Rudnev
School of Mathematics
University Walk
Bristol BS8 1TW, UK
E-mail: misarudnev@gmail.com

Ilya Shkredov
Steklov Mathematical Institute
Gubkina 8
119991 Moscow, Russia
and IITP RAS
Bolshoy Karetny per. 19
127994 Moscow, Russia
and MIPT
Institutskii per. 9
141701 Dolgoprudnii, Russia
E-mail: ilya.shkredov@gmail.com

Yuri Shteinikov
SRISA
Nahimovsky prosp. 36, building 1
117218 Moscow, Russia
E-mail: yuriisht@gmail.com