ISSN 2220-5438

Reprint from

Moscow Journal of Combinatorics and Number Theory

Volume 5 • Issue 1–2 2015

МФТИ

URSS

Moscow Journal of Combinatorics and Number Theory
Volume 5 • Issue 1–2 2015
URSS

Moscow Journal
of Combinatorics
and Number Theory
2015, vol. 5, iss. 1–2,
pp. 52–69

A bound on the multiplicative energy of a sum set and extremal sum-product problems

Oliver Roche-Newton (Linz) and Dmitry Zhelezov (Gothenburg)

Abstract: In recent years some near-optimal estimates have been established for certain sum-product type estimates. This paper gives some first extremal results which provide information about when these bounds may or may not be tight. The main tool is a new result which provides a nontrivial upper bound on the multiplicative energy of a sum set or difference set.

Keywords: Primitive roots, finite fields, Sidon sets, difference sets

AMS Subject classification: 11N69, 11A07, 11N25

Received: 05.10.2014; **revised:** 17.10.2014

1. Introduction

A now familiar variation on the Erdős-Szemerédi sum-product problem is the following: given a set $X(A)$ which is defined via a combination of additive and multiplicative operations on an input set A, show that the set $X(A)$ is always "large" compared to the original set A.

An example of a relatively old result of this type is due to Ungar [20], who showed that any finite [1)] set P of points in the plane determines at least $|P| - 1$ different pairwise directions, provided that the point set does not lie on a single line.

[1)] From now on, all sets are assumed to be finite unless stated otherwise.

If one then applies this bound in the case when $P = A \times A$, where A is an arbitrary set of real numbers such that $|A| \geq 2$, it follows that

$$\left|\frac{A-A}{A-A}\right| \geq |A|^2 - 2, \tag{1.1}$$

where

$$\frac{A-A}{A-A} := \left\{\frac{a-b}{c-d} : a, b, c, d \in A, c \neq d\right\}. \tag{1.2}$$

This notation for defining sets in terms of additive and multiplicative operations will be used flexibly throughout the paper; for example $A(A+A) := \{a(b+c) : a, b, c \in A\}$. Whenever the definition includes division, it is stipulated that we do not divide by zero, as in (1.2).

In recent years we have seen some more progress in this direction, thanks largely to progress in the field of discrete geometry. For example, it was recently established in [2] that for any subset A of the positive reals,

$$\left|\frac{A+A}{A+A}\right| \geq 2|A|^2 - 1. \tag{1.3}$$

It was also proven in [2] that the same result holds when $A \subset \mathbb{C}$, albeit with a smaller and unspecified multiplicative constant in the place of 2. Similarly, it was established in [9] that

$$|A(A+A+A+A)| \gg \frac{|A|^2}{\log |A|} \tag{1.4}$$

holds for any set $A \subset \mathbb{C}$ [2)].

Furthermore, building on the work of Guth and Katz [7], it was established in [10] that

$$|(A-A)(A-A)| \gg \frac{|A|^2}{\log |A|}, \tag{1.5}$$

and the same argument also works to prove that $|(A+A)(A+A)| \gg |A|^2/\log |A|$.

In the form of inequalities (1.1), (1.3), (1.4) and (1.5), we are seeing some progress relating to the sum-product problem. In particular, each of these four

[2)] Throughout this paper, for positive values X and Y the notation $X \gg Y$ is used as a shorthand for $X \geq cY$, for some absolute constant $c > 0$.

inequalities is optimal up to constant and logarithmic factors, as can be seen by taking $A = \{1, 2, \dots, |A|\}$. Once we have optimal estimates for such problems, it seems natural to ask the question: "under what circumstances can these results be tight?".

Each of (1.1), (1.3), (1.4) and (1.5) can be close to tight in the more general case when A has small sum set (i. e. when $|A+A| \leq c|A|$ for an absolute constant c). However, we are not aware of any other constructions which exhibit the tightness of these bounds. We make the following conjecture:

Conjecture 1.1 *There exist absolute constants c and c' such that for any $A \subset \mathbb{C}$*

$$\left|\frac{A+A}{A+A}\right| \leq c|A|^2 \Rightarrow |A+A| \leq c'|A|.$$

Similar conjectures can be made for the sets $\frac{A-A}{A-A}$, $A(A+A+A+A)$ and $(A-A)(A-A)$. In this paper, we prove some weak first results in the direction of Conjecture 1.1 and variants thereof. For example, we prove the following result:

THEOREM 1. *There exists an absolute constant $C > 0$ such that if $A \subset \mathbb{C}$ satisfies $\left|\frac{A+A}{A+A}\right| \ll |A|^2$, then*

$$|A+A| \ll |A|^2 \exp\left(-C\log^{1/3-\epsilon}|A|\right).$$

The same result holds with any of $\frac{A-A}{A-A}$, $(A+A)(A+A)$ or $(A-A)(A-A)$ in the place of $\frac{A+A}{A+A}$. It is interesting to note that if we assume the following variation of the sum-product conjecture, namely that

$$\max\{|A+A|, |A/A|\} \gg |A|^{2-o(1)}, \tag{1.6}$$

we can get another conditional bound relevant to Conjecture 1.1. Indeed, let $|A+A| = |A|^{1+\delta}$ for some $\delta > 0$ and $B = A+A$. Then, by the Plünnecke-Ruzsa inequality,

$$|B+B| \ll |A|^{1+4\delta}$$

and

$$|B/B| \ll |A|^2$$

by the hypothesis of the conjecture. Thus, if $0 < \delta < 1/2$ the set B violates (1.6). In other words, if we assume that the full sum-product conjecture holds and

$\left|\frac{A+A}{A+A}\right| \ll |A|^2$, then either $|A+A| \ll |A|$ or $|A+A| \gg |A|^{3/2-o(1)}$. So in fact Theorem 1 estimates the sum set size from the *opposite* side to what one would expect from sum-product type estimates. Unfortunately, the best exponent for the sum-product proved to date is $4/3 - o(1)$ (see [18]), which gives only trivial unconditional estimates for the above argument. [3)]

The new tool here which leads to Theorem 1 and its variants is an upper bound on the multiplicative energy of a sum set or difference set. The *multiplicative energy of* A, denoted $E^*(A)$, is the number of solutions to the equation

$$ab = cd, \quad (a,b,c,d) \in A^4. \tag{1.7}$$

The notion of multiplicative energy has played a key role in several of the most recent works on the sum-product problem, most notably in the work of Solymosi [18] in bounding the multiplicative energy in terms of the sum set, and consequently deducing what stands as the best estimate towards the Erdős-Szemerédi conjecture.

Since fixing a, b and c in (1.7) determines [4)] d, a trivial upper bound is given by $E^*(A) \leq |A|^3$. Combining this with the trivial upper bound $|A+A| < |A|^2$, we note that a trivial upper bound for the multiplicative energy of a sum set is given by $E^*(A+A) \leq |A|^6$. We give a small improvement to this upper bound as follows.

THEOREM 2. *For any $\epsilon > 0$ there are constants $C'(\epsilon), C''(\epsilon) > 0$ such that for any set $A \subset \mathbb{C}$*

$$E^*(A-A) \leq \max\left\{C''(\epsilon)|A|^{3+\epsilon}, |A-A|^3 \exp\left(-C'(\epsilon)\log^{1/3-\epsilon}|A|\right)\right\}.$$

In particular, there is a constant $C(\epsilon) > 0$ such that [5)]

$$E^*(A-A) \ll |A|^6 \exp\left(-C\log^{1/3-\epsilon}|A|\right).$$

[3)] Since this paper was originally submitted, an improvement was made towards the Erdős- Szemerédi conjecture in [8]. The best exponent for the original sum-product problem now stands as $4/3 + c$, for a small positive constant c.

[4)] Here we are making the simplifying assumption that $0 \notin A$. However, there are also at most $4|A|^2$ solutions to (1.7) which include a zero somewhere, and so we can still write $E^*(A) \ll |A|^3$ if it is the case that $0 \in A$.

[5)] In fact, one can replace ϵ with a $\log\log^{O(1)}$ factor and then the constant C becomes absolute.

Once Theorem 2 has been established, it is an easy corollary to show that the same bounds hold for the quantity $E^*(A+A)$.

The proof of Theorem 2 uses some heavy machinery from (additive) number theory, in the form of the Subspace Theorem, the Freiman Inverse Theorem and the Balog-Szemerédi-Gowers Theorem. The proof is based on work of Schwartz [15], who used the Subspace Theorem to give estimates for a variant on the Erdős unit distance problem. See also [16] and [17] for some similar combinatorial applications of the Subspace Theorem. Some similar results to Theorem 2 are proven in [21] with the roles of addition and multiplication reversed. Non-trivial bounds for the additive energy $E^+(AA)$ are established, although some extra conditions on A are needed.

Once Theorem 2 has been established, all that is required is an application of the Cauchy—Schwarz inequality to prove some initial results in the direction of Conjecture 1.1 as outlined above.

It can be calculated that if A is a geometric progression of the form $A = \{2^n : 1 \leq n \leq |A|\}$, then $E^*(A+A) \gg |A|^5$. The authors are unaware of any examples of sets A for which $E^*(A+A)$ is significantly greater than $|A|^5$, and it would be interesting to close the gap between $|A|^5$ and $o(|A|^6)$ in either direction.

In section 2 we will give the proof of Theorem 2, and give the details of the calculation which shows that it is possible that $E^*(A+A) \gg |A|^5$. In section 3, Theorem 1 and its variants are deduced as a corollary of Theorem 2, and we will also use an application of the Szemerédi-Trotter Theorem to prove a quantitatively improved version of Theorem 1 with $A(A+A+A+A)$ in place of $\frac{A+A}{A+A}$.

2. Multiplicative energy of sum and difference sets

2.1. Proof of Theorem 2

The key ingredient of the proof of Theorem 2 is the following lemma, which says that a difference set cannot contain a large number of elements from a multiplicative group of small rank.

LEMMA 1. *Let $\epsilon > 0$. Then there are positive constants $c(\epsilon), C(\epsilon)$ such that for any set A of complex numbers the following holds. For any multiplicative group $\Gamma \subset \mathbb{C}^*$ of rank $c(\epsilon)\log|A|$, the number of pairs*

$$\{(a_1, a_2) \in A \times A \mid a_1 - a_2 \in \Gamma\}$$

is at most $C(\epsilon)|A|^{1+\epsilon}$.

The proof of Lemma 1 is essentially an adaptation of the argument of Schwartz [15] and Schwartz, Solymosi, de Zeeuw [17] which they used in order to attack the Erdős unit distance problem for configurations of points with a group structure. In turn, their argument relies on a powerful tool from number theory, namely the Subspace Theorem. It seems that it was first introduced to the field of arithmetic combinatorics by Chang in [3]. The Subspace Theorem has a few different formulations and the one we will use is due to Evertse, Schlickewei and Schmidt [6] with the quantitative bounds due to Amoroso and Viada [1].

Suppose $a_1, \dots, a_k \in \mathbb{C}^*$ and

$$\Gamma = \{\alpha_1^{z_1} \cdots \alpha_r^{z_r}, z_i \in \mathbb{Z}\},$$

so Γ is a free multiplicative group [6)] of rank r. Consider the equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1 \tag{2.1}$$

with $a_i \in \mathbb{C}^*$ viewed as fixed coefficients and $x_i \in \Gamma$ as variables. A solution $(x_1, \dots, x_k)$ to (2.1) is called *nondegenerate* if for any non-empty $J \subsetneq \{1, \dots, k\}$

$$\sum_{i \in J} a_i x_i \neq 0.$$

THEOREM 3 (THE SUBSPACE THEOREM). *The number $A(k, r)$ of nondegenerate solutions to* (2.1) *satisfies the bound*

$$A(k, r) \leq (8k)^{4k^4(k+kr+1)}. \tag{2.2}$$

PROOF. (of Lemma 1) We start by constructing a graph G with the vertex set identified with A and placing an edge between two vertices a_1 and a_2 if and only if $a_1 - a_2 \in \Gamma$. Without loss of generality we assume that $-1 \in \Gamma$ and so if $x \in \Gamma$, $-x \in \Gamma$ as well. Thus, we consider G as an unoriented graph. The number of elements in the set of edges $E(G)$ is then half of the number of pairs (a_1, a_2) such that $a_1 - a_2 \in \Gamma$. Our strategy is thus to show that $|E(G)|$ cannot be too large.

Indeed, any path of length k between two vertices b_1 and b_2 in G, when rescaled, gives a solution to (2.1), so the number of paths is controlled by the

[6)] The original theorem is formulated in a more general setting, namely for the division group of Γ, but we will stick to the current formulation for simplicity.

Subspace Theorem. The only problem to overcome is the degeneracy condition, which is addressed below. The calculations turn out to be similar to the proof of Theorem 2 in [15], and essentially we merely observe that the proof in [15] does not utilise the hypothesis that the pairs are separated by distance 1. However, we decided to present the argument in full to make the proof more self-contained.

We proceed in a few steps.

Let $n = |A| = |V(G)|$ and $|E(G)| = n^{1+\epsilon}$ for some fixed $\epsilon > 0$. The rank r of Γ is $c(\epsilon)\log n$ with $c(\epsilon)$ to be defined in due course. We will show that provided $c(\epsilon)$ is small enough, n cannot be arbitrarily large.

Step 1. We prune G so that the minimal degree $\delta(G)$ is at least $\frac{1}{2}n^{\epsilon}$. We simply remove one by one vertices with degree less than $\frac{1}{2}n^{\epsilon}$. Since we can remove at most $\frac{1}{2}n^{1+\epsilon}$ edges, for the resulting graph G' we have $\frac{1}{2}n^{1+\epsilon} \leq |E(G')|$. We reassign the label G to this graph G'.

Step 2. Let $k \geq 1$ be an integer parameter to be chosen later. Any non-closed (but not necessarily simple) path $\langle v_1, \dots, v_k \rangle$ in G gives rise to the identity

$$(v_1 - v_2) + \cdots + (v_{k-1} - v_k) = v_1 - v_k,$$

and since $(v_i, v_{i+1}) \in E(G)$ we have $x_i := v_i - v_{i+1} \in \Gamma$. Then, dividing by $v_1 - v_k$ we get a solution to an equation of the type (2.1). However, in order to use the Subspace Theorem, we have to make sure such a solution is non-degenerate. Let us call a path non-degenerate if it gives a non-degenerate solution in the way we have just described.

Let us fix a vertex v and estimate the number of non-degenerate k-paths emanating from v. We build a path by adding each edge one by one while keeping the path non-degenerate. Since $\delta(G) \geq \frac{1}{2}n^{\epsilon}$, at each step we have at least that many edges to choose from, but for those making the path degenerate. The maximal number of such "bad" edges after l vertices have been chosen is $2^l - 1$, so the total number of non-degenerate k-paths P_v emanating from v is at least

$$P_v \geq \prod_{l=0}^{k-1} \left(\frac{1}{2}n^{\epsilon} - 2^l + 1 \right) \geq \frac{n^{k\epsilon}}{2^{2k}},$$

provided $n^{\epsilon} \geq 2^{k+2}$. There are at most n vertices in $V(G)$ and so by pigeonholing there is some vertex $w \in V(G)$ such that there are at least

$$\frac{n^{\epsilon k-1}}{2^{2k}} \tag{2.3}$$

non-degenerate k-paths between v and w.

Step 3. Now we can apply the Subspace Theorem. Combining the bounds (2.2) and (2.3) and taking logs, we have

$$\begin{aligned}(\epsilon k-1)\log n \leq (4k^5+4k^5r+4k^4)\log(8k)+k\log 4 < \\ < 5k^5 r\log(8k) = c(\epsilon)5k^5\log(8k)\log n.\end{aligned} \tag{2.4}$$

In order for the last inequality in (2.4) to hold, it is sufficient to assume that $r > 16$. But we can take $k = \lceil \frac{2}{\epsilon} \rceil$ and $c(\epsilon) = (5\log(8k)k^5)^{-1}$, which implies that (2.4) gives a contradiction. It must be the case that one of the assumptions $n^{\epsilon} \geq 2^{k+2}$ or $r > 16$ does not hold. In other words, it must be the case that $n < n_0(\epsilon)$ for some finite n_0. We finish the proof by taking the constant $C(\epsilon) = n_0$. □

Another powerful and well-known tool is the (Freiman)-Green—Ruzsa theorem which describes sets with small doubling. It has long been known that sets with small doubling are very similar to generalised arithmetic progressions of bounded rank, but until recently the quantitative bounds were rather weak. However, in a series of breakthrough papers Schoen, Croot and Sisask, Sanders (see [14], [4], [12]) [7], to name a few, gradually improved the bounds to almost best possible. We refer the reader to [11] for an excellent exposition.

We need some technical definitions in order to formulate the Freiman—Green—Ruzsa theorem for arbitrary abelian groups. Let G be such an abelian group with the operation written additively. A *d-dimensional centred convex progression* $P \subset G$ is defined as an image of a symmetric convex body $Q \subset \mathbb{R}^d$ under a homomorphism $\phi : \mathbb{Z}^d \to G$, so that $\phi(\mathbb{Z}^d \cap Q) = P$.

The quantitative version of the Freiman—Green—Ruzsa theorem with the state of the art bounds is formulated as follows (see Theorem 1.4 in [11] and references therein).

[7] Of course, we are not even trying to make a comprehensive list of contributors. Instead, we refer the interested reader to [11].

THEOREM 4. *Suppose that $|A+A| \leq K|A|$. Then there is a set X, a finite subgroup H and a d-dimensional centred convex progression P such that*

$$A \subset X + H + P$$

and the following bounds[8] *hold*

$$|X| \leq \exp(C \log^{3+o(1)} K) \tag{2.5}$$

$$d \leq C \log^{3+o(1)} K \tag{2.6}$$

$$|H + P| \leq \exp(C \log^{3+o(1)} K)|A|. \tag{2.7}$$

In our case we are interested only in subsets lying inside subgroups of bounded rank, so we record the following corollary.

COROLLARY 1. *Let $A \subset \mathbb{C}^*$ with $|AA| < K|A|$. Then there is $A_1 \subset A$ such that*

$$|A| \exp(-C \log^{3+o(1)} K) \leq |A_1|$$

and A_1 is contained in a multiplicative group of rank at most $C \log^{3+o(1)} K$, where C is a positive absolute constant.

PROOF. By Theorem 4,

$$A \subset X \cdot H \cdot P,$$

where the same notation is used. Since H is a finite subgroup, it is generated by a root of unity. Since $P = \phi(\mathbb{Z}^d \cap Q)$ for some homomorphism ϕ, it is contained in the subgroup generated by $\phi(e_1), \ldots, \phi(e_d)$, where the e_i are the standard basis elements. So, P is contained in a subgroup of rank d. Finally, there is an $x \in X$ such that $|xH \cdot P \cap A| \geq |A|/|X|$ and since $\{xH \cdot P\}$ is generated by at most $d+2$ elements, it follows that $A_1 = \{xH \cdot P\} \cap A$ satisfies the desired conditions by Theorem 4. □

The last tool that will be needed for the proof of Theorem 2 is the following version of the Balog—Szemerédi-Gowers theorem due to Schoen [13].

[8] Here $o(1)$ is just a shortening for a $\log\log^{O(1)} K$ factor, rather than an asymptotic notation, see [11].

THEOREM 5. *Let A be a subset of an abelian group, written additively, such that $E^+(A) = |A|^3/K$. Then there exists $A' \subset A$ such that $|A'| \gg |A|/K$ and*

$$|A' - A'| \ll K^4|A'|.$$

In particular, by the Plünnecke-Ruzsa inequality,

$$|A' + A'| \ll K^8|A'|.$$

Now we return to the proof of Theorem 2.

PROOF OF THEOREM 2.

Let $B = A - A$ and $E^*(B) = |B|^3/K$. Applying the Balog—Szemerédi-Gowers theorem multiplicatively, we obtain the subset $B' \subset B$ such that $|B'| \gg |B|/K$ and $|B'B'| \ll K^8|B'|$. By Corollary 1, there is $B'' \subset B'$ of size at least $|B'| \cdot \cdot \exp(-C\log^{3+o(1)} K)$ contained in a multiplicative group of rank r at most $C \cdot \cdot \log^{3+o(1)} K$.

Let us fix $1/100 > \epsilon > 0$, $c(\epsilon)$ and $C(\epsilon)$ given by Lemma 1 and denote these numbers by c_1 and C_1 respectively. Denote also $C'(\epsilon) = c_1/C$; it can be assumed that $C' \leq 1$, since otherwise we can take a sufficiently small value of $c_1(\epsilon)$ and Lemma 1 also holds for this value. Let us assume that

$$\log K \leq C' \log^{1/3-\epsilon} |A|,$$

so that in particular

$$\begin{aligned} r &\leq C(C')^{3+o(1)} \log|A| \leq \\ &\leq CC' \log|A| = \\ &= c_1 \log|A|. \end{aligned}$$

Then, we have $|B''| \leq C_1|A|^{1+\epsilon}$ by Lemma 1. Expanding the inequalities, we have

$$\begin{aligned} E^*(B) = \frac{|B|^3}{K} &\ll \\ &\ll K^2|B'|^3 \leq \\ &\leq K^2 \exp(3C\log^{3+o(1)} K)|B''|^3 \leq \end{aligned}$$

$$\leq K^2 \exp(3C \log^{3+o(1)} K) C_1 |A|^{3+3\epsilon} \leq$$
$$\leq \exp(2C' \log^{1/3-\epsilon} |A|) \exp(3CC' \log^{1-\epsilon/2} |A|) C_1 |A|^{3+3\epsilon} \leq$$
$$\leq C''(\epsilon) |A|^{3+4\epsilon},$$

by our assumptions on K. Otherwise, if $\log K \geq C' \log^{1/3-\epsilon} |A|$, we have

$$E^*(B) \leq |A - A|^3 \exp(-C' \log^{1/3-\epsilon} |A|). \tag{2.8}$$

Taking ϵ small enough, we conclude that for arbitrarily small $\epsilon > 0$ there exist constants $C'(\epsilon), C''(\epsilon) > 0$ such that

$$E^*(A - A) \leq \max \left\{ C''(\epsilon) |A|^{3+\epsilon}, |A - A|^3 \exp\left(-C'(\epsilon) \log^{1/3-\epsilon} |A|\right) \right\}. \tag{2.9}$$ □

The next task is to record a corollary of Theorem 2, namely that the same result holds for $E^*(A + A)$.

THEOREM 6. *For any $\epsilon > 0$ there is a positive constant $C'(\epsilon)$ such that for any set $A \subset \mathbb{C}$*

$$E^*(A + A) \ll_\epsilon \max \left\{ |A|^{3+\epsilon}, (|A - A|^3 + |A + A|^3) \exp\left(-C'(\epsilon) \log^{1/3-\epsilon} |A|\right) \right\}.$$

In particular, there is a constant $C(\epsilon) > 0$ such that

$$E^*(A + A) \ll |A|^6 \exp\left(-C \log^{1/3-\epsilon} |A|\right).$$

PROOF. Write $B = A \cup -A$ and note that $A + A \subset B - B$. It follows from this inclusion that $E^*(A + A) \leq E^*(B - B)$. Now apply Theorem 2 for the set B. Since $|B| \leq 2|A|$ and $|B - B| \ll |A + A| + |A - A|$, the desired conclusion follows. □

2.2. A set whose sum set has large multiplicative energy

To conclude this section, let us give more details of the calculation which shows that for $A = \{2^n : n \in \{1, \ldots, |A|\}\}$, we have $E^*(A + A) \gg |A|^5$. Let us assume for simplicity of exposition that $|A|$ is a multiple of 3.

The quantity $E^*(A+A)$ is the number of solutions to $s_1s_2 = s_3s_4$ such that $s_i \in A+A$. However, since A is a Sidon set, this is exactly the same as the number of solutions to

$$(2^{n_1} + 2^{n_2})(2^{n_3} + 2^{n_4}) = (2^{n_5} + 2^{n_6})(2^{n_7} + 2^{n_8}) \tag{2.10}$$

such that $n_1, \dots, n_8 \in \{1, \dots, |A|\}$. After expanding the brackets (2.10) becomes

$$2^{n_1+n_3} + 2^{n_1+n_4} + 2^{n_2+n_3} + 2^{n_2+n_4} = 2^{n_5+n_7} + 2^{n_5+n_8} + 2^{n_6+n_7} + 2^{n_6+n_8}. \tag{2.11}$$

We will show that there are at least $\left(\frac{|A|}{3}\right)^5$ "trivial" solutions to (2.11), corresponding to octuples $(n_1, \dots, n_8) \in [|A|]^8$ which satisfy the system of equations

$$n_1 + n_3 = n_5 + n_7, \tag{2.12}$$

$$n_1 + n_4 = n_5 + n_8, \tag{2.13}$$

$$n_2 + n_3 = n_6 + n_7, \tag{2.14}$$

$$n_2 + n_4 = n_6 + n_8. \tag{2.15}$$

To see this, simply choose any combination of five elements $n_1, \dots, n_5$ from the middle third interval $\{\frac{|A|}{3}, \frac{|A|}{3} + 1, \cdots, \frac{2|A|}{3} - 1\}$. Then the octuple

$$(n_1, n_2, n_3, n_4, n_5, n_2 + n_5 - n_1, n_1 + n_3 - n_5, n_1 + n_4 - n_5) \in [|A|]^8$$

satisfies the aforementioned system of equations. Indeed, (2.12) and (2.13) follow straight away from the choice of n_7 and n_8 in the above octuple. It remains to check that (2.14) and (2.15) hold. This is indeed the case, since

$$\begin{aligned} n_6 &= n_2 + n_5 - n_1 = \\ &= n_2 + n_3 - (n_1 + n_3 - n_5) = \\ &= n_2 + n_3 - n_7 \end{aligned}$$

and similarly

$$\begin{aligned} n_6 &= n_2 + n_5 - n_1 = \\ &= n_2 + n_4 - (n_1 + n_4 - n_5) = \\ &= n_2 + n_4 - n_8. \end{aligned}$$

The choices of $n_1, \dots, n_5$ were made arbitrarily from a subset of $[|A|]$ of size $|A|/3$, and so it follows that we have at least $\left(\frac{|A|}{3}\right)^5$ solutions to (2.11). This confirms that $E^*(A+A) \gg |A|^5$.

3. Structural sum-product estimates

3.1. Proof of Theorem 1

By the Cauchy—Schwarz inequality,

$$E^*(B)|B/B| \gg |B|^4 \tag{3.1}$$

for any set $B \subset \mathbb{C}$. Applying this inequality with $B = A + A$, and then using the hypothesis that $\left|\frac{A+A}{A+A}\right| \ll |A|^2$, it follows that

$$|A+A|^4 \ll \left|\frac{A+A}{A+A}\right| E^*(A+A) \ll |A|^2 E^*(A+A).$$

Applying Theorem 6, we have

$$|A+A|^4 \ll |A|^8 \exp(-C \log^{1/3-\epsilon} |A|),$$

for some constant C, from which the desired conclusion that $|A+A| \ll |A|^2 \cdot$ $\cdot \exp(-C' \log^{1/3-\epsilon} |A|)$ follows. □

It is straightforward to exchange $\frac{A+A}{A+A}$ with $(A+A)(A+A)$ in the above proof. To do this, simply use a slightly different version of (3.1) in the form of

$$E^*(B)|BB| \gg |B|^4.$$

Furthermore, it is a straightforward task to modify the proof of Theorem 1 by taking $B = A - A$ and using Theorem 2 instead of Theorem 6, in order to obtain matching result for products and ratios of difference sets. We summarise these remarks as well as Theorem 1 in the following theorem:

THEOREM 7. *There exists a positive absolute constant C such that for any finite set $A \subset \mathbb{C}$, each of the following statements holds*:

(*i*) *if* $\left|\frac{A+A}{A+A}\right| \ll |A|^2$ *then* $|A+A| \ll |A|^2 \exp(-C\log^{1/3-\epsilon}|A|)$;

(*ii*) *if* $|(A+A)(A+A)| \ll |A|^2$ *then* $|A+A| \ll |A|^2 \exp(-C\log^{1/3-\epsilon}|A|)$;

(*iii*) *if* $\left|\frac{A-A}{A-A}\right| \ll |A|^2$ *then* $|A-A| \ll |A|^2 \exp(-C\log^{1/3-\epsilon}|A|)$;

(*iv*) *if* $|(A-A)(A-A)| \ll |A|^2$ *then* $|A-A| \ll |A|^2 \exp(-C\log^{1/3-\epsilon}|A|)$.

Another way to express similar results building from Theorem 2 is to state that a set A with very small product set will determine a set $(A+A)(A+A)$ (as well as other variations with different combinations of addition/subtraction and multiplication/division as in Theorem 7) which satisfies $|(A+A)(A+A)| = \omega(|A|^2)$.

Here is a short sketch of this argument. If $|AA| \leq K|A|$ for an absolute constant K, we can apply a result of Chang [3] to deduce that $|A+A| \gg |A|^2$. See also [16, Theorem 11] for an exposition of the result of Chang. Then, if we repeat the arguments of the proof of Theorem 1, applying Theorem 2 and the Cauchy—Schwarz inequality, it follows that

$$|(A+A)(A+A)| \gg |A|^2 \exp(C\log^{1/3-\epsilon}|A|),$$

which breaks the $|A|^2$ threshold for sets with very small product set [9].

3.2. Using the Szemerédi-Trotter Theorem

In this subsection, the Szemerédi-Trotter Theorem will be used to prove a version of Theorem 1 for the set $A(A+A+A+A)$. Recall that the Szemerédi-Trotter Theorem is the following.

THEOREM 8 (THE SZEMERÉDI-TROTTER THEOREM). *Given a set P of points and a family L of lines in $\mathbb{R}^2$, the set of incidences $I(P,L) := \{(p,l) \in P \times L : p \in l\}$ satisfies*

$$|I(P,L)| \ll |P|^{2/3}|L|^{2/3} + |P| + |L|.$$

The Szemerédi-Trotter Theorem has a long association with the sum-product problem. The relationship was initiated by the work of Elekes [5], who used Theo-

[9] We are grateful to Brendan Murphy for helping to bring this to our attention.

rem 8 to give a short proof that $\max\{|A+A|, |AA|\} \gg |A|^{5/4}$. Since then, incidence geometry has been used as a tool in proving several sum-product inequalities, including the proof of (1.4).

We will use Theorem 8 to prove the following lemma. Although the proof is standard, and similar result have been referenced in the literature, it seems that the full statement and proof have not been published in their entirety, and so a proof is given here for completeness. A version of this result with the roles of multiplication and addition reversed was set as Exercise 8.3.3 in [19].

LEMMA 2. *Let $A \neq \{0\}$ be a subset of $\mathbb{R}$ and let B and C be any sets of real numbers such that $B + C \neq \{0\}$. Then*

$$|A(B+C)| \gg (|A||B||C|)^{1/2}.$$

PROOF. Let $A^* = A \setminus \{0\}$, and note that it follows from the assumption on the set A that A^* is non empty, and thus $|A^*| \gg |A|$. Let $l_{a,b}$ denote the line with equation $y = a(x+b)$, and let

$$L := \{l_{a,b} : a, b \in A^* \times B\}.$$

By ensuring that a is non-zero, we have $|L| = |A^*||B| \gg |A||B|$. Let $P = C \times \times A(B+C)$, and note that each line $l_{a,b} \in L$ has at least $|C|$ incidences with P, since for all $c \in C$,

$$(c, a(b+c)) \in P \cap l_{a,b}.$$

Therefore, $|I(P,L)| \gg |A||B||C|$, and then by the Szemerédi-Trotter theorem

$$|A||B||C| \ll (|A||B||C||A(B+C)|)^{2/3} + |C||A(B+C)| + |A||B|. \tag{3.2}$$

If $|C| \ll 1$ then $|A(B+C)| \geq |A(B+c)| \gg |A|^{1/2}|B|^{1/2} \gg (|A||B||C|)^{1/2}$ for some [10] $c \in C$. Therefore, we can assume that the third term in (3.2) is irrelevant and thus

$$|A||B||C| \ll (|A||B||C||A(B+C)|)^{2/3} + |C||A(B+C)|. \tag{3.3}$$

[10] The inequality $A(B+c) \gg |A|^{1/2}|B|^{1/2}$ uses the non-degeneracy condition that $B + C \neq \{0\}$ and therefore there is some $c \in C$ such that $B + c \neq \{0\}$.

Depending on which of the two terms on the RHS of (3.3) is dominant, we have either $|A(B+C)| \gg (|A||B||C|)^{1/2}$ or $|A(B+C)| \gg |A||B|$, that is,

$$|A(B+C)| \gg \min\{(|A||B||C|)^{1/2}, |A||B|\}. \tag{3.4}$$

Finally, one can interchange the roles of B and C in the proof of (3.4) to establish that

$$|A(B+C)| \gg \min\{(|A||B||C|)^{1/2}, |A||C|\}, \tag{3.5}$$

and since $(|A||B||C|)^{1/2}$ cannot dominate both $|A||B|$ and $|A||C|$, the proof is complete. □

We are now ready to use this lemma to prove a structural result for $|A(A+A+ + A+A)|$.

THEOREM 9. *If* $|A(A+A+A+A)| \ll |A|^2$ *then* $|A+A| \ll |A|^{3/2}$.

PROOF. Applying Lemma 2 with $B = C = A+A$, as well as the assumption that $|A(A+A+A+A)| \ll |A|^2$, it follows that

$$|A+A||A|^{1/2} \ll |A(A+A+A+A)| \ll |A|^2.$$

Simply rearranging this gives $|A+A| \ll |A|^{3/2}$ as claimed. □

Remark. In fact, is easy to modify the proof of Theorem 9 to get the same result with the set $(A+A)(A+A+A)$ in the place of $A(A+A+A+A)$ [11].

Acknowledgements

Oliver Roche-Newton was supported by the Austrian Science Fund (FWF): Project F5511-N26, which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". Part of this research was undertaken when the authors were visiting the Institute for Pure and Applied Mathematics, UCLA, which is funded by the NSF. We are grateful to Brandon Hanson, Nets Katz, Brendan Murphy, Ilya Shkredov and Jozsef Solymosi for several helpful conversations related to the content of this paper.

[11] We are grateful to Ilya Shkredov for bringing this to our attention.

Bibliography

1. ***F. Amoroso, E. Viada***, *Small points on subvarieties of a torus*, Duke Math. J. **150**:3 (2009), 407–442.
2. ***A. Balog, O. Roche-Newton***, *New sum-product estimates for real and complex numbers*, Discrete Comput. Geom. **53**:4 (2015), 825-846.
3. ***M. C. Chang***, *Sums and products of different sets*, Contrib. Discrete Math. **1**:1 (electronic) (2006), 47–56.
4. ***E. Croot, O. Sisask***, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. **20**:6 (2010), 1367–1396.
5. ***G. Elekes***, *On the number of sums and products*, Acta Arith. **81** (1997), 365–367.
6. ***J.-H. Evertse, H. P. Schlickewei, W. M. Schmidt***, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. **155**:3 (2002), 807–836.
7. ***L. Guth, N. H. Katz***, *On the Erdős distinct distance problem in the plane*, Ann. of Math. 181:1 (2015), 155-190.
8. ***S. Konyagin, I. Shkredov***, *On sum sets of sets, having small product set*, arxiv:1503.0577 (2015).
9. ***B. Murphy, O. Roche-Newton, I. Shkredov***, *Variations on the sum-product problem*, SIAM J. Discrete Math. **29**:1 (2015), 514-540.
10. ***O. Roche-Newton, M. Rudnev***, *On the Minkowski distances and products of sum sets*, to appear in Israel J. Math., arxiv:1203.6237 (2012).
11. ***T. Sanders***, *The structure theory of set addition revisited*, Bull. Amer. Math. Soc. (N.S.) **50**:1 (2013), 93–127.
12. ***T. Sanders***, *On the Bogolyubov–Ruzsa lemma*, Anal. PDE **5**:3 (2012), 627–655.
13. ***T. Schoen***, *New bounds in Balog–Szemeredi-Gowers theorem*, preprint available at http://www.staff.amu.edu.pl/schoen/remark-B-S-G.pdf.
14. ***T. Schoen***, *Near optimal bounds in Freimans theorem*, Duke Math. J. **158**:1 (2011), 1–12.
15. ***R. Schwartz,*** *Using the Subspace Theorem to bound unit distances*, arxiv:1211.4948 (2012).
16. ***R. Schwartz, J. Solymosi***, *Combinatorial applications of the Subspace Theorem*, arxiv:1311.3734 (2013).
17. ***R. Schwartz, J. Solymosi, F. de Zeeuw***, *Rational distances with rational angles*, Mathematika **58** (2012), 409–418.
18. ***J. Solymosi***, *Bounding multiplicative energy by the sumset*, Adv. Math. **222** (2009), 402–408.
19. ***T. Tao, V. Vu***, *Additive combinatorics*, Cambridge University Press (2006).

20. ***P. Ungar***, $2N$ *non collinear points determine at least* $2N$ *directions*, J. Combin. Theory Ser. A **33** (1982), 343–347.

21. ***D. Zhelezov***, *On sets with small additive doubling in product sets*, J. Number Theory, **153** (2015), 170–183.

O. Roche-Newton

Wuhan University,
Wuhan, Hubei Province,
P.R.China, 430072
o.rochenewton@gmail.com

D. Zhelezov

Chalmers University of Technology and University of Gothenburg,
Gothenburg, Sweden, 41296
zhelezov@chalmers.se