



AUSTRIAN
ACADEMY OF
SCIENCES

Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

RICAM
JOHANN-RADON-INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

Higher convexity and iterated sum sets

B. Hanson, O. Roche-Newton, M. Rudnev

RICAM-Report 2020-41

HIGHER CONVEXITY AND ITERATED SUM SETS

BRANDON HANSON, OLIVER ROCHE-NEWTON, AND MISHA RUDNEV

ABSTRACT. Let f be a smooth real function with strictly monotone first k derivatives. We show that for a finite set A , with $|A + A| \leq K|A|$,

$$|2^k f(A) - (2^k - 1)f(A)| \gg_k |A|^{k+1-o(1)} / K^{O_k(1)}.$$

We deduce several new sum-product type implications, e.g. that $A + A$ being small implies unbounded growth for a many enough times iterated product set $A \cdots A$.

1. INTRODUCTION

When A is a subset of an Abelian group, define its sumsets via

$$A + A = \{x_1 + x_2 : x_1, x_2 \in A\},$$

and

$$mA - nA = \{(x_1 + \cdots + x_m) - (x_{m+1} + \cdots + x_{m+n}) : x_1, \dots, x_{m+n} \in A\}.$$

Additive combinatorics is interested in the cardinality and structure of sumsets. Now suppose $A = \{a_1 < \dots < a_N\}$ is a set of real numbers, listed in increasing order. The sequence of first differences has terms

$$a_{i+1} - a_i, \quad 1 \leq i \leq N - 1,$$

and when this sequence is strictly increasing, we say A is *convex*. Erdős posed the problem of estimating $|A + A|$ when A is convex. It is no loss of generality to assume $A = f([N])$, where $[N] = \{1, \dots, N\}$ and f is a differentiable function with strictly increasing first derivative.

The first non-trivial lower bound was given by Hegyvári [9]. Following Elekes's introduction of incidence geometry to sum-product type problems in [4], results concerning sum set estimates for convex A were generalised by Elekes, Nathanson and Ruzsa in [5]:¹

Theorem 1.1 (Elekes, Nathanson and Ruzsa). *Let $A, B, C \subset \mathbb{R}$ and let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a strictly convex function. Then,*

$$(1) \quad |A + B|^2 |f(A) + C|^2 \gg |A|^3 |B| |C|.$$

In particular, if A is a convex set then $|A + A| \gg |A|^{3/2}$.

¹We shall use throughout the notation $X \ll Y$ to mean $X \leq CY$ for some absolute constant C . Writing $X \ll_k Y$ means there is a constant C_k which depends only on k such that $X \leq C_k Y$. All the sets, denoted by uppercase letters are finite, of cardinality $|\cdot|$.

The current record is due to Shkredov [17], building up on work of Schoen and Shkredov from [16]. If A is convex, then

$$|A + A| \gg \frac{|A|^{58/37}}{(\log |A|)^{20/37}}, \quad |A - A| \gg \frac{|A|^{8/5}}{\log^{2/5} |A|}.$$

The right-hand side of both inequalities has been improved by Olmezov [11] to $|A|^{5/3}$ under additional assumptions on the signs of third and fourth derivatives of the convex function f , with $A = f([N])$. Olmezov develops on the method of Garaev [8], which is elementary: it relies only on basic combinatorics and order. The same is true of this paper and the bulk of [15], from which we draw our inspiration.

A related result, appearing in [15], establishes the following theorem in a simple but remarkably effective manner.

Theorem 1.2 (Ruzsa, Shakan, Solymosi, Szemerédi). *For a convex $A \subset \mathbb{R}$, one has*

$$|2A - A| \gg |A|^2.$$

In this article we develop upon the elementary considerations underlying the above result. In a sense, Theorem 1.2 cannot be improved: take $A = \{n^2 : 1 \leq n \leq N\}$. However, if one had a set A which was “more” convex than the first N perfect squares one might hope for more, and indeed this is the first generalisation we establish. In what follows, it will be easier to think of A as a sequence, in increasing order. We say $A = \{a_1 < \dots < a_N\}$ is 1-convex if it is convex, and inductively we say A is k -convex if its sequence of first differences $\{a_{i+1} - a_i\}$ are $(k-1)$ -convex. Thus, $\{n^2 : 1 \leq n \leq N\}$ is 1-convex, while $\{n^3 : 1 \leq n \leq N\}$ is 2-convex, and $\{2^n : 1 \leq n \leq N\}$ is k -convex for any $k \leq N-1$.

The foundation of our paper is the following generalisation of Theorem 1.2.

Theorem 1.3. *Let $k \geq 2$ be an integer and let A be a k -convex sequence. Then*

$$|2^k A - (2^k - 1)A| \gg \frac{|A|^{k+1}}{2^{k^2}}.$$

We note here that a small modification of the forthcoming proof of Theorem 1.3 gives a better dependence on the constant k , replacing the 2^{k^2} in the denominator with $k!$. However, we present this slightly weaker bound in order to align its proof with that of Theorem 1.4, our main result.

The form of the result of Elekes, Nathanson and Ruzsa stated in (1) may be viewed as a generalisation of the sum-product phenomenon. It implies, for instance, that at least one of $|A + A|$ and $|f(A) + f(A)|$ must be large. Indeed, Theorem 1.1 implies that if A is a finite set of real numbers satisfying $|A + A| \leq K|A|$, and f is a convex function, then

$$|f(A) + f(A)| \gg \frac{|A|^{3/2}}{K}.$$

Our main theorem extends Theorem 1.3 into a statement in the spirit of this inequality. For an interval I , we say $f : I \rightarrow \mathbb{R}$ is 0-convex function if it is strictly monotone on I , and in general, f is k -convex on I if each of the derivatives $f^{(1)}, f^{(2)}, \dots, f^{(k+1)}$ exists and is non-vanishing on I (hence all but the last one are strictly monotone).

Theorem 1.4. *Let A be a finite set of real numbers contained in an interval I and let f be function which is k -convex on I for some $k \geq 1$. Suppose that $|A| > 10k$. Then if $|A + A - A| \leq K|A|$, we have*

$$|2^k f(A) - (2^k - 1)f(A)| \geq \frac{|A|^{k+1}}{(CK)^{2^{k+1}-k-2} (\log |A|)^{2^{k+2}-k-4}},$$

for some absolute constant $C > 0$.

By applying Theorem 1.4 to various choices of f , we obtain theorems about iterated growth in the spirit of the renown Erdős-Szemerédi sum-product problem. Finite sets $A \subset \mathbb{R}$ defining few distinct products are known to yield arbitrarily large iterated sumsets for sufficiently many iterations: this constitutes the so-called FPMS (few products, many sums) phenomenon. See e.g. [3], [10], [2], [18] and the references contained therein. Among these, the results by Shkredov [18] apply to non-ordered fields as well, for they are based on geometric incidence estimates which hold true over general fields. In contrast, we make a point of avoiding geometric incidence theory here but use order in an essential way, as is the case in [2], [3], and [10]. An application of our Theorem 1.4 gives the iterated sums growth comparable to [3] and [10] but is weaker than [2]. However, the above-mentioned papers rely quite heavily on the Distributive Law, and their results are therefore specific to the FPMS setup.

Theorem 1.4, however, is sufficiently general so as to produce bounds for other sum-product type iterated growth questions that have not, to our knowledge, been established before.

Corollary 1.5. *For all $k \geq 1$ and $\varepsilon > 0$, there exists $\delta = \delta(k, \varepsilon) > 0$ such that, for any sufficiently large finite set of positive real numbers A , the following hold:*

(1) *If $|A + A| \leq |A|^{1+\delta}$, then we have*

$$|(A^{2^{k-1}} \cdots A) / (A^{2^{k-1}-1} \cdots A)| \gg |A|^{k-\varepsilon}.$$

(2) *If $|AA| \leq |A|^{1+\delta}$, then we have*

$$|((A+1)^{2^{k-1}} \cdots (A+1)) / ((A+1)^{2^{k-1}-1} \cdots (A+1))| \gg |A|^{k-\varepsilon}.$$

(3) *If $|A + A| \leq |A|^{1+\delta}$ and $A^k = \{a^k : a \in A\}$ for some integer $k \geq 2$, then we have*

$$|2^{k-1} A^k - (2^{k-1} - 1) A^k| \gg |A|^{k-\varepsilon}.$$

The same is true if a^k is replaced by any polynomial in a of degree k , or any real (positive or negative) power of a distinct from $0, \dots, k-1$, provided it is well-defined.

Further applications in light of some questions existing in the literature are left to Section 4.

We conclude this introduction with a few remarks. First, Theorem 1.4 highlights that it is not only exponentiation that disrupts additive structure, which is the basis for the sum-product problem, but in fact any non-linear function which does not oscillate too wildly on the interval containing A . Indeed, if f is sufficiently differentiable and any of its first $k+1$ derivatives has a controlled number of zeroes, then, by the pigeonhole principle, one can pass to a reasonably large subset of A which avoids them all.

Second, while the dependence on k and K in Theorem 1.4 is hardly optimal, the theorem tells us that the condition that f be k -convex is necessary and sufficient in order to produce a lower bound of the form $|A|^{k+1}$. Indeed, the k 'th powers $\{n^k : 1 \leq n \leq N\}$ can be seen to grow like N^k under iterated sums and differences, but not beyond. On the other hand, incidence geometry techniques for convex functions, initiated in [5] and based on the Szemerédi-Trotter theorem, seem not to distinguish between convexity and higher convexity.

Finally, we point out that Theorem 1.4 gives new information in the context of the 3-fold sum-product problem. The resulting inequality

$$(2) \quad \max\{|A + A - A|, |AA/A|\} \gg \frac{|A|^{3/2}}{(\log |A|)^{3/2}}$$

appears to be stronger than the previously known best 3-fold sum-product bounds.

2. PROOF OF THEOREM 1.3

The proof is a natural extension of that of Theorem 1.2 which we will recall. To proceed we introduce some notation. Let $\Delta a_i = a_{i+1} - a_i$, so Δ is the forward difference operator. In this notation, Theorem 1.2 follows from the observation that

$$(3) \quad a_i < a_i + \Delta a_j < a_{i+1}$$

for $j < i$. The latter condition is guaranteed by insisting that $j < N/2 < i$, which is the condition we will adopt in our proof.

Proof of Theorem 1.3. At the expense of a constant factor, we may assume that $|A| = 2^l - 1$, for some l , by truncating A if necessary. We proceed by induction on k . We will in fact show that the set $2^k A - (2^k - 1)A$ contains at least $|A|^{k+1}2^{-k^2}$ elements in the interval $(\min(A), \max(A))$, this stronger statement being better suited to induction. The base case of this induction is Theorem 1.2, and follows immediately from inequality (3).

For the inductive step, we let

$$(\Delta A)' = \{a_2 - a_1 < \dots < a_{2^{l-1}} - a_{2^{l-1}-1}\}$$

and

$$(\Delta A)'' = \{a_{2^{l-1}+1} - a_{2^{l-1}} < \dots < a_{2^l-1} - a_{2^l-2}\}.$$

For $i \geq 2^{l-1}$, the set $a_i + (\Delta A)'$ is a subset of the interval (a_i, a_{i+1}) because

$$\max((\Delta A)') < \min((\Delta A)'') \leq a_{i+1} - a_i.$$

By induction $2^{k-1}(\Delta A)' - (2^{k-1} - 1)(\Delta A)'$ contains at least $(2^{l-1} - 1)^k 2^{-(k-1)^2}$ elements in the interval $(a_2 - a_1, a_{2^{l-1}} - a_{2^{l-1}-1})$. Thus we can find $(2^{l-1} - 1)^k 2^{-(k-1)^2}$ distinct elements in the interval $(a_i, a_{i+1}]$ from the set $a_i + 2^{k-1}(\Delta A)' - (2^{k-1} - 1)(\Delta A)'$. Since $(\Delta A)' \subseteq A - A$, we have produced a total of

$$(2^{l-1} - 1)(2^{l-1} - 1)^k 2^{-(k-1)^2} \geq |A|^{k+1} 2^{-k^2}$$

distinct elements from the set $2^k A - (2^k - 1)A$. \square

3. PROOF OF THEOREM 1.4

To motivate the proof of Theorem 1.4, which is a generalisation of the proof of Theorem 1.3, it is worth generalising Theorem 1.2 first. Let us assume for the moment that both f and f' are increasing.

A convex sequence is obtained by applying a convex function f to the interval $[N] = \{1, \dots, N\}$ to get $a_i = f(i)$. In this way, the inequalities

$$a_i < a_i + a_{j+1} - a_j \leq a_{i+1}$$

can be rewritten as

$$(4) \quad f(i) < f(i) + f(j+1) - f(j) < f(i+1).$$

The significance of adding 1 to the arguments of f is that 1 is a common consecutive difference of $[N]$. The quantity $f(j+1) - f(j)$ is suggestive of a derivative of f . Indeed, if f' is increasing then so is

$$(\Delta_h f)(x) := f(x+h) - f(x) = \int_0^h f'(x+t)dt$$

for any fixed $h > 0$.

Now the proof Theorem 1.2 allows us to deduce that if $A = \{a_1 < \dots < a_N\}$ has many distinct consecutive differences $a_{i+1} - a_i$, then $|A + A - A|$ is large. We can therefore use the bound $|A + A - A| \leq K|A|$, along with a dyadic pigeonhole argument, to deduce that many consecutive differences of A are oft-repeated. Once such a repeated difference, say h , is obtained, we can use that $\Delta_h f$ is increasing to generate many inequalities of the form (4).

Throughout we shall write

$$H(A) = \{a_{j+1} - a_j : j = 1, \dots, N-1\}$$

for the set of consecutive differences of A , and for $h \in H(A)$, we write

$$A_h = \{a_i : a_{i+1} - a_i = h\}.$$

With this notation in hand, if f' is increasing and $a_i, a_j \in A_h$ for some $j < i$ then

$$(5) \quad f(a_i) < f(a_i) + f(a_j + h) - f(a_j) \leq f(a_i + h),$$

generalising (4). If f were decreasing, we would instead have

$$(6) \quad f(a_i + h) < f(a_i) - f(a_j + h) + f(a_j) \leq f(a_i),$$

and if $\Delta_h f$ were decreasing in either case, we would insist instead that $j > i$.

We will need the following dyadic pigeonhole lemma, which is a quantitative version of Theorem 1.2.

Lemma 3.1. *Let $A = \{a_1 < \dots < a_N\}$ be a set of reals and suppose N is sufficiently large. There is a set $H' \subseteq H(A)$ of size m and an integer L satisfying*

- (i) $Lm \geq N/(3 \log_2 N)$,
- (ii) $|A + A - A| \geq (Lm^2)/2$, and
- (iii) for each $h \in H'$, $L \leq |A_h| \leq 2L$.

Proof. Let

$$i(j) = 1 + |\{h \in H(A) : h < a_{j+1} - a_j\}|.$$

In other words, if $H(A) = \{h_1 < \dots < h_k\}$ is ordered, $i(a_{j+1} - a_j) = l$ if $a_{j+1} - a_j = h_l$ (so i is the index).

Moreover, since

$$a_j \leq a_j + h < a_{j+1}$$

for $h \in H \cup \{0\}$ with $h < a_{j+1} - a_j$, it follows that there are $i(j)$ elements of $A + A - A$ in the interval $[a_j, a_{j+1})$, whence

$$|A + A - A| \geq \sum_{j=1}^{N-1} i(j) = \sum_{l=1}^k l|i^{-1}(l)|.$$

For $0 \leq t \leq \log N$, let

$$I_t = \{l : 2^t \leq |i^{-1}(l)| < 2^{t+1}\}$$

Then

$$N - 1 = \sum_l |i^{-1}(l)| \leq 2 \sum_{t=0}^{\log_2 N} 2^t |I_t|,$$

so for some t we have

$$|I_t|2^t \geq \frac{N}{3 \log_2 N}.$$

From this,

$$\sum_{l=1}^k l|i^{-1}(l)| \geq \sum_{l \in I_t} l2^t \geq 2^{t-1} |I_t|^2.$$

We let $H' = \{h_l : l \in I_t\}$ and $L = 2^t$. \square

We now prove Theorem 1.4 in the case $k = 1$. This means showing that

$$|2f(A) - f(A)| \gg \frac{|A|^2}{K(\log |A|)^3}.$$

Applying Lemma 3.1, we obtain a subset $H' \subset H(A)$ of size m and an integer L . For $h \in H'$ and for $a_i, a_j \in A_h$ we can apply (5), provided $j < i$ and f' is increasing. This gives us $L^2/2$ different sums from $2f(A) - f(A)$ in the intervals $(f(a_i), f(a_i + h))$. These intervals are disjoint for distinct h as $a_i + h = a_{i+1}$ and f is increasing. Adding the contributions from different $h \in H'$, we have produced $mL^2/2$ distinct sums in $2f(A) - f(A)$. By (i) and (ii),

$$|2f(A) - f(A)| \gg \frac{(mL)^2}{m} \gg \frac{|A|^2}{K(\log |A|)^3}.$$

In the case that f or f' is decreasing, we can use inequality (6) or insist that $j > i$ as needed.

Before moving on to the general case of Theorem 1.4, we need a bit of notation. Recall that for $h_1 \in H(A)$ we write

$$A_{h_1} = \{a_i \in A : a_{i+1} - a_i = h_1\}.$$

Inductively, we define

$$A_{h_1, \dots, h_k} = (A_{h_1, \dots, h_{k-1}})_{h_k},$$

which means those elements $a \in A_{h_1, \dots, h_{k-1}}$ whose successor in $A_{h_1, \dots, h_{k-1}}$ is $a + h_k$. Similarly, we write

$$(\Delta_{h_1} f)(x) = f(x + h_1) - f(x)$$

and inductively define

$$(\Delta_{h_1, \dots, h_k} f)(x) = (\Delta_{h_1, \dots, h_{k-1}} f)(x + h_k) - (\Delta_{h_1, \dots, h_{k-1}} f)(x).$$

Lemma 3.2. *Let f be a k -convex function on $[a, b]$. Then for any h with $0 < h < b - a$, $\Delta_h f$ is $(k-1)$ -convex on $[a, b-h]$. In particular, if $j \leq k$ and $h_1, \dots, h_j > 0$ then $\Delta_{h_1, \dots, h_j} f$ is strictly monotone.*

Proof. The first claim holds as

$$(\Delta_h f)^{(l)}(x) = f^{(l)}(x + h) - f^{(l)}(x) = \int_0^h f^{(l+1)}(x + t) dt,$$

and if $l \leq k$ then the integrand on the right has fixed sign, and so the sign of the left hand side is fixed as well. It follows that $\Delta_{h_1, \dots, h_j} f$ is $(k-j)$ -convex, and since $k-j \geq 0$, this means its derivative is non-vanishing. \square

Proof of Theorem 1.4. We will prove the statement by induction on k , with the further conclusion that all sums produced lie in the interval $(\min(f(A)), \max(f(A)))$. We will assume that f and f' are both increasing, as the case where either of them is decreasing is handled similarly. The constant C will be chosen so as to close the induction, and may change from

line to line. We have already established the case $k = 1$. So assume the statement holds for $k - 1$ and any set A with corresponding value of K .

Apply Lemma 3.1 to obtain a set $H' \subset H(A)$ of size m such that for each $h \in H'$ we have a set A_h of size $N_h \geq L$. Now write

$$A_h = \{a_1 < \dots < a_{N_h}\}.$$

The function $\Delta_h f$ is increasing and so the values $\Delta_h f(a_i)$ are as well. Let

$$A'_h = \{a_i : i \leq N_h/2\}, \quad A''_h = \{a_i : i \geq N_h/2\}.$$

Then we have the containment

$$f(a_i) + \Delta_h f(A'_h) \subset (f(a_i), f(a_i + h))$$

for each $a_i \in A''_h$. But the left hand side is the image of A'_h under the function $g = f(a_i) + \Delta_h f$. The function g is $(k - 1)$ -convex on $(\min(A'_h), \max(A'_h))$ by Lemma 3.2. Now

$$|A'_h + A'_h - A'_h| \leq |A + A - A| \leq K|A| \leq (CK^2(\log |A|)^2)|A'_h|,$$

by properties (i) and (ii) of Lemma 3.1. So by induction there are at least

$$T = \frac{L^k}{(CK^2(\log |A|)^2)^{2^k-k-1}(\log |A|)^{2^{k+1}-k-3}}$$

distinct elements from

$$2^{k-1}g(A_h) - (2^{k-1} - 1)g(A_h) \subseteq 2^k f(A) - (2^k - 1)f(A)$$

in the interval $(f(a_i), f(a_i + h))$. Now

$$L \geq \frac{|A|}{Cm \log |A|} \geq \frac{|A|}{CK(\log |A|)^2}$$

so that

$$T \geq \frac{|A|^k}{C^{2^k-1}K^{2^{k+1}-k-2}(\log |A|)^{2^{k+2}-k-5}}.$$

This induction now applies to each $a_i \in A''_h$, independently for each $h \in H'$, and the elements of $2^k f(A) - 2^{k-1} f(A)$ constructed belong to disjoint sub-intervals of $(\min(A), \max(A))$. The total number of elements constructed is

$$LmT \gg \frac{|A|}{C \log |A|} \cdot \frac{|A|^k}{C^{2^k-1}K^{2^{k+1}-k-2}(\log |A|)^{2^{k+2}-k-5}} = \frac{|A|^{k+1}}{C^{2^k}K^{2^{k+1}-k-2}(\log |A|)^{2^{k+2}-k-4}}$$

and the induction closes for appropriately large C . \square

4. APPLICATIONS

Of particular relevance in this section is the following general form of the Erdős-Szemerédi sum-product conjecture [7]: for all $\varepsilon > 0$ and every integer $k \geq 2$ there exists a constant $c = c(k, \varepsilon) > 0$ such that for all $A \subset \mathbb{N}$

$$\max\{|kA|, |A^{(k)}|\} \geq c|A|^{k-\varepsilon}.$$

In the above inequality, $A^{(k)}$ denotes the k -fold product set

$$A^{(k)} = \{x_1 \cdots x_k : x_1, \dots, x_k \in A\}.$$

The conjecture is widely believed to hold in the more general setting of $A \subset \mathbb{R}$. The question is wide open even in the most studied the case of $k = 2$. Little is known for larger values of k , with the exception of the milestone FPMS-paper by Bourgain and Chang [1] for sets of natural numbers, whose results were recently reproved in a beautiful way and somewhat strengthened by Pálvolgyi and Zhelezov [12].

In order to make significant progress with these difficult problems, it is necessary at least to understand what happens in the extreme case when one of the sum set or product set is small. But even with this strong additional information, not everything is clear, especially over \mathbb{R} . There has been progress in proving that few products implies many iterated sums, and it is known that $|kA|$ grows arbitrarily large when $|AA| \leq K|A|$ and K is small (in particular, effective results are known for $K = |A|^\varepsilon$ for $\varepsilon > 0$ sufficiently small). The best result (over \mathbb{R}) in this direction is due to Bush and Croot [2].

4.1. Few sums implies many iterated products. Our first application concerns product sets of A when the sum set is small. For $k = 2$ an optimal result

$$|A + A| \leq K|A| \Rightarrow |AA| \geq |A|^{2-\varepsilon}K^{-C}$$

follows from a simple application of the Szemerédi-Trotter Theorem. See [6], where $C = 4$; it is possible to lower it down to $8/3$. It is not obvious how to iterate this to get bigger growth for more products, and even the result

$$|A + A| \leq K|A| \Rightarrow |AAA| \geq |A|^{2+\varepsilon}K^{-C}$$

was proved only recently [13].

Theorem 1.4 implies the following result that *few sums implies unbounded iterated products*, part (1) of Corollary 1.5.

Proof of Corollary 1.5, (1). Let $f(x) = \log(x)$ and note that f and all of its derivatives are non-zero on $(0, \infty)$. Apply Theorem 1.4 with this function f , which is k -convex for any k .

By the Plünnecke inequality

$$|A + A - A| \leq |A|^{1+3\delta}.$$

9

Theorem 1.4 therefore gives

$$|2^k f(A) - (2^k - 1)f(A)| \gg \frac{|A|^{k+1}}{(C|A|^{3\delta})^{2^{k+1}-k-2}(\log |A|)^{2^{k+2}-k-4}}.$$

By taking δ to be sufficiently small with respect to ε and k , the denominator above can be made smaller than $|A|^\varepsilon$, provided A is sufficiently large. Since $f(A) = \log(A)$, sums of $f(A)$ correspond with products of A , and the statement follows. \square

4.2. Products and shifts. An important variant of the sum-product phenomenon is the idea that additive perturbations destroy multiplicative structure. For instance, consider the following result of Shkredov [18]: for all finite $A \subset \mathbb{R}$,

$$(7) \quad |AA|^4|(A+1)(A+1)| \gg \frac{|A|^6}{\log |A|}.$$

In particular, if $|AA| \leq K|A|$ it follows that the shifted product set $(A+1)(A+1)$ is close to maximal in size. Note that the value of the shift in (7) can be replaced by an arbitrary non-zero λ by applying the inequality to $\lambda^{-1} \cdot A$.

Similar statements to (7) can be deduced from results on convexity and sum sets. For instance, let $X \subset \mathbb{R}$ and apply (1) with

$$A = \log(X) = B, C = \log(X+1), f(x) = \log(e^x + 1)$$

it follows that

$$|AA|^2|(A+1)(A+1)|^2 \gg |A|^5.$$

Theorem 1.4 gives similar statement about iterated growth, which is (2) of Corollary 1.5.

Proof of Corollary 1.5, (2). Let $B = \log A$, then using Plünnecke's inequality, we have

$$|B + B - B| \leq |B|^{1+3\delta}.$$

Let $f(x) = \log(1 + e^x)$. Calculating derivatives of f shows that f is k -convex for any k . It therefore follows that

$$|(A+1)^{(2^k)} / (A+1)^{(2^k-1)}| = |2^k f(B) - (2^k - 1)f(B)| \geq \frac{|A|^{k+1}}{(C|A|^{3\delta})^{2^{k+1}-k-2}(\log |A|)^{2^{k+2}-k-4}}.$$

By taking δ to be sufficiently small with respect to ε and k , the denominator is at most $|A|^\varepsilon$, as required. \square

We anticipate future applications of the ideas in this paper to give new results about growth of products under shifts and further consequences. We present one application here, which is an analogue of the main result from [13], and gives a positive answer to a question raised in [14].

Theorem 4.1. *Let A be a set of positive reals and suppose that $|AA| \leq K|A|$. Then there are positive constants c, C such that*

$$|(A+1)(A+1)(A+1)| \gg \frac{|A|^{2+c}}{K^C}.$$

Proof. This argument closely follows the proof of Theorem 3.2 in [13], and a slightly more detailed account can be found there. The important new information comes from an application of Theorem 1.4.

Claim. *Let $A \subset \mathbb{R}$ and $|AA| \leq K|A|$. Then*

$$(8) \quad \left| \frac{(A+1)(A+1)(A+1)(A+1)}{(A+1)(A+1)(A+1)} \right| \gg \frac{|A|^3}{K^{18}(\log |A|)^{14}}$$

Proof. Apply Theorem 1.4 with $k = 3$ and

$$B = \log A, \quad f(x) = \log(e^x + 1).$$

Then $|B + B - B| = |AA/A|$ and $|4f(B) - 3f(B)| = |(A+1)^{(4)}/(A+1)^{(3)}|$. The claim follows. \square

Further applications of Plünnecke-Ruzsa give

$$\begin{aligned} \frac{|A|^3}{K^{18}(\log |A|)^{14}} &\ll \left| \frac{(A+1)(A+1)(A+1)(A+1)}{(A+1)(A+1)(A+1)(A+1)} \right| \leq \frac{|(A+1)(A+1)(A+1)(A+1)|^4}{|(A+1)(A+1)|^3} \\ &\leq \frac{|(A+1)(A+1)(A+1)|^{16}}{|(A+1)(A+1)|^{15}} \end{aligned}$$

It follows from an application of (7) that

$$|(A+1)(A+1)(A+1)|^{16} \gg \frac{|A|^{33}}{K^{78}(\log |A|)^{29}},$$

which completes the proof. \square

4.3. $|A + A|$ versus $|A^k + A^k|$. Raising the elements of A to a power ought to disrupt any additive structure present in the set A . As in the preceding sections, we can deduce Corollary 1.5 part (3) from Theorem 1.4.

Proof of Corollary 1.5, (3). Using the Plünnecke inequality, we have $|A + A - A| \leq |A|^{1+3\varepsilon}$. We deduce the conclusion by applying Theorem 1.4 to A with the function $f(x) = x^k$. The same is true if x^k is replaced by any power of x other than $0, \dots, k-1$.

If $f(x)$ is instead a polynomial of degree k then f and its derivatives combine for at most $k!$ roots. We can select a subset A' of size $|A|/k!$ which lies in an interval not containing any of these roots, and adjust ε if necessary to overcome the factor $k!$. \square

The number of sums and differences of k 'th powers here is an important problem. The case where K is minimized, i.e. where $A = [N]$, reduces to Waring's problem. In this setting, quantitative questions become far more delicate. This is highlighted by the fact that even in the simplest case $k = 3$ and $A = [N]$, the true order of magnitude of $|A + A + A|$ is unknown. The best result is $|A + A + A| \gg N^{3\beta}$ with $\beta = 0.91709477$, due to Wooley [19].

ACKNOWLEDGEMENTS

Oliver Roche-Newton was partially supported by the Austrian Science Fund FWF Project P 30405-N32. Misha Rudnev is partially supported by the Leverhulme Trust Grant RPG-2017-371. We are grateful to Antal Balog, Peter Bradshaw, Brendan Murphy and Audie Warren for helpful discussions.

REFERENCES

- [1] J. Bourgain and M.-C. Chang, ‘On the size of k -fold sum and product sets of integers’, *J. Amer. Math. Soc.* 17 (2004), 473–497.
- [2] A. Bush and E. Croot, ‘Few products, many h -fold sums’, *International Journal of Number Theory* 14 (2018), no. 8, 2107–2128.
- [3] E. Croot and D. Hart, ‘ h -fold sums from a set with few products’, *SIAM J. Discrete Math.* 24 (2010), no. 2, 505–519.
- [4] G. Elekes, ‘On the number of sums and products’, *Acta Arith.* 81 (1997), 365–367.
- [5] G. Elekes, M. Nathanson and I. Ruzsa, ‘Convexity and sumsets’, *J Number Theory* 83 (1999), 194–201.
- [6] G. Elekes and I. Ruzsa, ‘Few sums, many products’, *Studia Scientiarum Mathematicarum Hungarica* 40 (2003), 301–308.
- [7] P. Erdős, E. Szemerédi, ‘On sums and products of integers,’ Studies in pure mathematics, 213–218, Birkhäuser, Basel, 1983.
- [8] M. Garaev, On lower bounds for the L_1 -norm of exponential sums, *Mathematical Notes* 68 (2000), 713–720.
- [9] N. Hegyvári, ‘On consecutive sums in sequences’, *Acta Math. Acad. Sci. Hungar.* 48 (1986), 193–200.
- [10] L. Li, ‘Multi-fold sums from a set with few products’, arXiv:1106.6074.
- [11] K. Olmezov, ‘Additive properties of slowly growing convex sets’ (Russian), to appear in *Mat. Zametki*, 110, (2021) no. 6, 1–18.
- [12] D. Pálvolgyi and D. Zhelezov, ‘Query complexity and the polynomial Freiman-Ruzsa conjecture’, arXiv:2003.04648.
- [13] O. Roche-Newton and I. D. Shkredov, ‘If $A + A$ is small then AAA is superquadratic’, *J. Number Theory* 201 (2019), 124–134.
- [14] O. Roche-Newton and A. Warren, ‘New expander bounds from affine group energy’, *To appear in Disc. Comput. Geom.*
- [15] I. Z. Ruzsa, G. Shakan, J. Solymosi and E. Szemerédi, ”On distinct consecutive differences”, arXiv:1910.02159(2019).
- [16] T. Schoen and I. Shkredov, ‘On sumsets of convex sets’, *Combin. Probab. Comput.* 20 (2011), no. 5, 793–798.
- [17] I. Shkredov, ‘On sums of Szemerédi-Trotter sets’, *Proc. Steklov Inst. Math.* 289:1 (2015), 300309.
- [18] I. Shkredov, ‘Some remarks on sets with small quotient set’, *Mat. Sb.* 208 (2017), no. 12, 144–158.
- [19] T. D. Wooley, ‘Sums of three cubes, II’, *Acta Arith.* 170 (2015), no. 1, 73–100.

UNIVERSITY OF GEORGIA, ATHENS, GA, USA
E-mail address: brandon.w.hanson@gmail.com

JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, LINZ, AUSTRIA
E-mail address: o.rochenewton@gmail.com

UNIVERSITY OF BRISTOL, BRISTOL, UK
E-mail address: misharudnev@gmail.com