Convexity, Squeezing, and the Elekes-Szabó Theorem

Oliver Roche-Newton[a] Elaine Wong[b]

Submitted: Jun 15, 2022; Accepted: Nov 24, 2023; Published: Jan 12, 2024

Abstract

This paper explores the relationship between convexity and sum sets. In particular, we show that elementary number theoretical methods, principally the application of a squeezing principle, can be augmented with the Elekes-Szabó Theorem in order to give new information. Namely, if we let $A \subset \mathbb{R}$, we prove that there exist $a, a' \in A$ such that

$$\left| \frac{(aA+1)^{(2)}(a'A+1)^{(2)}}{(aA+1)^{(2)}(a'A+1)} \right| \gtrsim |A|^{31/12}.$$

We are also able to prove that

$$\max\{|A+A-A|, |A^2+A^2-A^2|, |A^3+A^3-A^3|\} \gtrsim |A|^{19/12}.$$

Both of these bounds are improvements of recent results and takes advantage of computer algebra to tackle some of the computations.

Mathematics Subject Classifications: 05B10, 05D99, 11B13

1 Introduction

We choose to begin with some boring stuff up front in order to avoid any awkwardness between us that may originate from cultural differences in mathematical notation. Throughout this paper, the notation $X \gg Y$, $Y \ll X$, $X = \Omega(Y)$, and $Y = O(X)$ are all equivalent and mean that $X \geqslant cY$ for some absolute constant $c > 0$. $X \approx Y$ and $X = \Theta(Y)$ denote that both $X \gg Y$ and $X \ll Y$ hold. $X \gg_a Y$ means that the implied constant is no longer absolute, but depends on a. We also use the notation $X \gtrsim Y$ and $Y \lesssim X$ to denote that $X \gg Y/(\log Y)^c$ for some absolute constant $c > 0$. Unless

[a] Institute for Algebra, Johannes Kepler University, Linz, Austria. (o.rochenewton@gmail.com)

[b] CSMD, Oak Ridge National Laboratory, Oak Ridge, TN, USA. (wongey@ornl.gov)

E. Wong acknowledges that this manuscript has been partially authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy (DOE). The publisher acknowledges the US government license to provide public access under the DOE Public Access Plan.

https://doi.org/10.37236/11331

otherwise stated, all logarithms are in base 2 and we will use the notation ℓn for logs in base e.

Now for the fun stuff. An important generalization of the sum-product phenomenon is the idea that strictly convex or concave functions destroy additive structure.[1] For instance, Elekes, Nathanson, and Ruzsa [5] used incidence geometry to prove that the bound

$$|A+A|^2|f(A)+f(A)|^2 \gg |A|^5$$

holds for any $A \subset \mathbb{R}$ and any strictly convex function f.

A recent trend in this area of sum-product theory has seen elementary methods play a more prominent role. These elementary methods have their origins in the work of Ruzsa, Shakan, Solymosi, and Szemerédi [18], who gave a simple and beautiful proof of the fact that

$$|A+A-A| \gg |A|^2 \tag{1}$$

holds for any convex set $A \subset \mathbb{R}$. A set A is said to be (*strictly*) *convex* if it has strictly increasing consecutive differences. That is, if we write $A = \{a_1 < a_2 < \cdots < a_n\}$ then $a_i - a_{i-1} < a_{i+1} - a_i$ holds for all $2 \leqslant i \leqslant n-1$. Note that the bound (1) is optimal up to constant factors, as can be seen by taking $A = \{1, 4, \ldots, n^2\}$.

For the purposes of our work, we will apply an elementary "squeezing" method to two different number-theoretic problems. This method was the foundation for the proof of (1), and has already been further developed in a series of recent papers (see [1], [2], [8], [9], [13]).

1.1 Products and Shifts

The squeezing method was used in [9] to give lower bounds for expanders involving convex and 'superconvex' functions. Informally, a superconvex function is a strictly convex function which has a strictly convex first derivative (this notion was considered in much more detail in [8]). The following result was established in [9]: for any $X \subset \mathbb{R}$, there exist $x, x' \in X$ such that

$$\left|\frac{(xX+1)^{(2)}(x'X+1)^{(2)}}{(xX+1)^{(2)}(x'X+1)}\right| \gtrsim |X|^{5/2}. \tag{2}$$

The notation $U^{(k)}$ is used for the k-fold product set of U, that is,

$$U^{(k)} := \{u_1 \cdots u_k \colon u_1, \ldots, u_k \in U\}.$$

It is perhaps not obvious why the bound (2) has anything to do with convexity. However, this is in fact a special case of a more general result involving growth of the set $f(a+A)$ under addition, see [9, Theorem 2.6]. Then the bound (2) follows by considering the strictly convex function $f(x) = \ell\text{n}(e^x+1)$ and $A = \ell\text{n}\, X$. In this paper, we give an improved bound for this expander.

[1] For the sake of completeness, it can be assumed that a convexity result has an analogous concavity result and we will only mention the former in statements of theorems and in the proofs.

Theorem 1. *For any finite set $X \subset \mathbb{R}$, there exists $x, x' \in X$ such that*

$$\left|\frac{(xX+1)^{(2)}(x'X+1)^{(2)}}{(xX+1)^{(2)}(x'X+1)}\right| \gtrsim |X|^{31/12}.$$

The primary motivation for proving the bound (2) in [9] was that it could be used to give a better non-trivial lower bound for the number of dot products determined by a point set in the Euclidean plane. By using Theorem 1 in place of (2) in the analysis of [9], one can obtain a further quantitative improvement to the main result of [9]. However, we will not explore this in detail here. Rather, we choose to focus on highlighting the methods that allow us to improve the bound (2).

1.2 Two Convex Functions

In [8], the same squeezing technique was used to prove that

$$|A+A-A||f(A)+f(A)-f(A)| \gg \frac{|A|^3}{\log|A|} \tag{3}$$

holds for any $A \subset \mathbb{R}$ and any strictly convex function f. In particular, it follows that

$$\max\{|A+A-A|, |f(A)+f(A)-f(A)|\} \gtrsim |A|^{3/2}. \tag{4}$$

The bound (3) is also tight, up to constant and logarithmic factors, as is illustrated by the case when $A = [n]$ for some positive integer n and $f(x) = x^2$. Moreover, a recent paper of Bradshaw [1] removed the logarithmic factors from (3).

An interesting open problem is to give a version of (4) with an exponent strictly greater than 3/2. Although we are unable to give such a result, we do obtain an improvement by instead simultaneously considering two different convex functions.

Theorem 2. *For any $A \subset \mathbb{R}$,*

$$\max\{|A+A-A|, |A^2+A^2-A^2|, |A^3+A^3-A^3|\} \gtrsim |A|^{19/12}.$$

2 The Elekes-Szabó Theorem

We will prove Theorems 1 and 2 in the next two sections using a "squeezing" idea originating from [18]. However, we would first like to introduce an additional tool in the form of the Elekes-Szabó Theorem in order to make new quantitative progress with these problems. The Elekes-Szabó Theorem gives a bound for the size of the intersection of a Cartesian product and a suitably non-degenerate algebraic surface. The first non-trivial bound for this problem was given by Elekes and Szabó in [7]. We will use the most recent quantitative version of this result, which is due to Solymosi and Zahl [20], building on previous work of Raz, Sharir, and de Zeeuw [14].

Theorem 3. *Let $F \in \mathbb{R}[x,y,z]$ be a non-degenerate irreducible polynomial of degree d, such that none of the partial derivatives $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}$ vanish. Then, for all $A, B, C \subseteq \mathbb{R}$ such that $|A| \leqslant |B| \leqslant |C|$,*

$$|Z(F) \cap (A \times B \times C)| = O_d((|A||B||C|)^{4/7} + |B||C|^{1/2}). \tag{5}$$

In particular,

$$|Z(F) \cap (A \times B \times C)| = O_d(\max\{|A|, |B|, |C|\}^{12/7}).$$

We are often interested in the case when $|A| = |B| = |C| = n$, in which case (5) simplifies to become

$$|Z(F) \cap (A \times B \times C)| \ll_d n^{12/7}.$$

On the other hand, a simple construction of [12] shows the existence of a non-degenerate quadratic polynomial $F : \mathbb{R}^3 \to \mathbb{R}$ and a set A of cardinality n with

$$|Z(F) \cap (A \times A \times A)| \gg n^{3/2}.$$

Of course, to understand Theorem 3, one needs to know what it means for f to be non-degenerate.

Definition 4. A polynomial $F \in \mathbb{R}[x,y,z]$ is *degenerate* if there exists a one-dimensional sub-variety $Z_0 \subseteq Z(F)$ such that for all $v \in Z(F) \setminus Z_0$, there are open intervals $I_1, I_2, I_3 \subseteq \mathbb{R}$ and injective real-analytic functions $\phi_i : I_i \to \mathbb{R}$ with real-analytic inverses $(i = 1, 2, 3)$ such that $v \in I_1 \times I_2 \times I_3$ and for any $(x, y, z) \in I_1 \times I_2 \times I_3$, we have

$$(x, y, z) \in Z(F) \text{ if and only if } \phi_1(x) + \phi_2(y) + \phi_3(z) = 0\,.$$

Otherwise, we say that F is *non-degenerate.*

This definition is rather technical. However, it may be helpful for the reader to consider an example of a function for which Theorem 3 cannot hold (and which therefore must be degenerate). If we take $F(x, y, z) = x + y - z$ and $A = B = C = [n]$, then it is not difficult to check that

$$|\{(a, b, c) \in A \times B \times C : F(a, b, c) = 0\}| \gg n^2.$$

In this case, the surface $Z(F)$ is a hyperplane. Theorem 3 therefore tells us that this F must be degenerate. We can also see this by looking at Definition 4 directly; here we set $\phi_1(t) = \phi_2(t) = t$ and $\phi_3(t) = -t$. This construction can be modified in many ways. For instance, one can take $F(x, y, z) = x^2 + y^2 - z^2$ and $A = B = C = \{\sqrt{1}, \sqrt{2}, \dots, \sqrt{n}\}$. Or one can take $F(x, y, z) = xyz$ and $A = B = C = \{2^i : i \in \pm[n]\}$. These examples are based on the same common idea, that the surface is a kind of deformation of a hyperplane, and this is captured conveniently by Definition 4.

For the case when the expression $F(x, y, z) = 0$ can already be rearranged into the form $z = f(x, y)$ where f is a polynomial, the definition of non-degeneracy becomes more straightforward (see [15, Theorem 2]). However, for the general case, it is not always immediately obvious whether a given polynomial is degenerate or non-degenerate. To help with this task, we will use an idea introduced by Elekes and Rónyai, which is that non-degeneracy can be verified using the following derivative test [6]. We include a proof here for completeness, which is essentially taken from [7, Lemma 33].

Lemma 5. *Let $f : \mathbb{R}^2 \to \mathbb{R}$ be a bivariate twice-differentiable real function and let U be a nonempty open subset of* $\mathrm{Dom}(f) \setminus (\{f_y = 0\} \cup \{f_x = 0\})$*. Suppose that there exist (twice-differentiable) univariate real functions $\psi, \varphi_1, \varphi_2$ such that*

$$f(x, y) = \psi(\varphi_1(x) + \varphi_2(y)).$$

Then

$$\frac{\partial^2 (\ell\mathrm{n}\, |f_x/f_y|)}{\partial x \partial y} \tag{6}$$

is identically zero on U.

Proof. First, we can calculate the partial derivatives f_x and f_y using the chain rule to get

$$\begin{aligned} f_x &= \varphi_1'(x) \cdot \psi'(\varphi_1(x) + \varphi_2(y)), \\ f_y &= \varphi_2'(y) \cdot \psi'(\varphi_1(x) + \varphi_2(y)). \end{aligned}$$

Therefore,

$$\frac{f_x}{f_y} = \frac{\varphi_1'(x)}{\varphi_2'(y)}.$$

We can then calculate the form of (6). Our assumptions on the set U ensure that this expression can be evaluated for all $(x, y) \in U$. First, we can use the chain rule to calculate the partial derivative with respect to x. We obtain

$$\frac{\partial (\ell\mathrm{n}\, |f_x/f_y|)}{\partial x} = \frac{f_y}{f_x} \cdot \frac{\varphi_1''(x)}{\varphi_2'(y)} = \frac{\varphi_1''(x)}{\varphi_1'(x)}.$$

This function does not depend on y, and so differentiating with respect to y gives a function which is identically zero. We conclude that

$$\frac{\partial^2 (\ell\mathrm{n}\, |f_x/f_y|)}{\partial x \partial y}(x, y) = 0$$

for all $(x, y) \in U$, as required. □

In practice, Lemma 5 allows us to test the whether or not the polynomial $F(x, y, z)$ is degenerate by rearranging the expression $F(x, y, z) = 0$ into the form $z = f(x, y)$, computing the resulting expression (6), and checking whether it is identically zero on an open set of $\mathbb{R}^2$. This characterization will be used repeatedly, and so we record it in the form of the next lemma. The result is implicit in earlier work going back to [6], but since we are not aware of it being stated in this form, we give the full statement and its proof here.

Lemma 6. *Suppose that $F : \mathbb{R}^3 \to \mathbb{R}$ is a degenerate polynomial. Let $f(x, y)$ be a twice differentiable real function with f_x and f_y not identically zero such that*

$$z = f(x, y) \Leftrightarrow F(x, y, z) = 0. \tag{7}$$

Then there exists a nonempty open set $U \subset \mathbb{R}^2$ such that

$$\frac{\partial^2 \left(\ell\mathrm{n}\, |f_x/f_y|\right)}{\partial x \partial y}$$

is identically zero on U.

Proof. Since F is degenerate, there is some open neighborhood $I_1 \times I_2 \times I_3$ intersecting $Z(F)$, and some smooth functions φ_1, φ_2 and φ_3 with smooth inverses, such that, for all $(x, y, z) \in I_1 \times I_2 \times I_3$,

$$F(x, y, z) = 0 \Leftrightarrow \varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0. \tag{8}$$

Then, since φ_3 has a smooth inverse on I_3, we can define a new smooth function $\psi(t) = \varphi_3^{-1}(-t)$. The second equation in (8) is therefore equivalent to $z = \psi(\varphi_1(x) + \varphi_2(y))$. Making use of the hypothesis (7), it then follows from (8) that, for all $(x, y, z) \in I_1 \times I_2 \times I_3$,

$$\begin{aligned} z = f(x, y) \Leftrightarrow F(x, y, z) = 0 &\Leftrightarrow \varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0 \\ &\Leftrightarrow z = \psi(\varphi_1(x) + \varphi_2(y)). \end{aligned}$$

Therefore, for all $(x, y, z) \in I_1 \times I_2 \times I_3$, we have

$$f(x, y) = \psi(\varphi_1(x) + \varphi_2(y)).$$

Define

$$U := \{(x, y) \in I_1 \times I_2 : f(x, y) \in I_3\} \setminus (\{f_x = 0\} \cup \{f_y = 0\})$$

and note that U is open, since it is the intersection of three open sets. Also, U is nonempty, since there is some $(x, y, z) \in I_1 \times I_2 \times I_3$ such that $F(x, y, z) = 0$ and f_x and f_y are both not identically zero. It then follows from Lemma 5 that (6) is identically zero on U. □

The development of the Elekes-Szabó Theorem has largely been motivated by applications to problems in discrete geometry. See the survey of de Zeeuw [3] for more background on this problem and its applications. A recent paper of Roche-Newton [17] applied the Elekes-Szabó Theorem in order to prove new results in sum-product theory. The present paper is strongly influenced by the ideas in [17], which in turn takes ideas from [19] and [11].

3 Proof of Theorem 2

The proofs of Theorems 1 and 2 are similar in structure and are based on the same ideas. However, Theorem 1 involves an extra level of computational and algebraic difficulty. It is therefore logical to begin by proving Theorem 2 in order to introduce the main ideas in the easier setting.

In order to prove Theorem 2, we will first prove the following result, which may be of independent interest. For any $A, B \subset \mathbb{R}$ and $G \subset A \times B$, We use the notation

$$A +_G B := \{a + b : (a, b) \in G\}$$

for the sum set $A + B$ restricted to G.

Lemma 7. *For any $A \subset \mathbb{R}$ and $G \subset A \times A \setminus \{(a, a) : a \in A\}$,*

$$\max\{|A -_G A|, |A^2 -_G A^2|, |A^3 -_G A^3|\} \gg |G|^{7/12}. \tag{9}$$

Proof. The proof is similar to the proof of the main result of [17]. Write

$$C := A -_G A, \quad D := A^2 -_G A^2, \quad E := A^3 -_G A^3.$$

We will double count solutions to the system of equations

$$c = a - b, \tag{10}$$
$$d = a^2 - b^2, \tag{11}$$
$$e = a^3 - b^3, \tag{12}$$

such that $(a, b) \in G$ and $(c, d, e) \in C \times D \times E$. Define S to be the number of solutions to this system. A simple observation is that

$$S = |G| \tag{13}$$

since each pair $(a, b) \in G$ gives rise to a unique solution.

We seek to find a complementary upper bound for S via an application of Theorem 3. For each contribution to S, we can eliminate a and b from the system above. Together, (10) and (11) imply that

$$b = \frac{d - c^2}{2c}, \qquad a = \frac{d + c^2}{2c}.$$

Note that we do not need to worry about dividing by zero here, since G does not contain any diagonal pairs with $a = b$, i.e., $c \neq 0$. Substituting this information into (12) and rearranging gives

$$4ce = 3d^2 + c^4.$$

Next, define

$$F(x, y, z) := 4xz - 3y^2 - x^4.$$

We have thus deduced that every contribution (a,b,c,d,e) to S gives rise to a solution (c,d,e) to the equation $F(c,d,e)=0$. Furthermore, no triple (c,d,e) contributes more than once to S, since for fixed c and d with $c \neq 0$ there exists at most one pair (a,b) which satisfies both (10) and (11). Therefore, we have

$$S \leqslant |Z(F) \cap C \times D \times E|. \tag{14}$$

Claim 8. *F is non-degenerate.*

Assuming that the claim is correct, we can apply Theorem 3 to obtain the upper bound

$$|Z(F) \cap C \times D \times E| \ll \max\{|C|,|D|,|E|\}^{12/7}.$$

Combining this with (14) and (13), we have

$$|G| \ll \max\{|C|,|D|,|E|\}^{12/7}$$

and it follows that

$$\max\{|C|,|D|,|E|\} \gg |G|^{7/12},$$

as required. It remains to prove the claim.

Proof of Claim. The expression $F(x,y,z)=0$ can be rearranged into the form

$$z = \frac{1}{4} \cdot \frac{3y^2+x^4}{x}.$$

We define

$$f(x,y) := \frac{1}{4} \cdot \frac{3y^2+x^4}{x}.$$

Suppose for a contradiction that F is degenerate. Then it follows from Lemma 6 that there is an open set $U \subset I_1 \times I_2$ on which (6) is identically zero. We can calculate (6) directly and obtain a contradiction. Indeed,

$$\frac{\partial^2 \left(\ell\text{n}\,|f_x/f_y|\right)}{\partial x \partial y} = \frac{8x^3y^2}{(x^4-y^4)^2}.$$

This is zero if and only if (x,y) is a point on the coordinate axes other than the origin, that is, if (x,y) belongs to the set

$$\{(x,0) : x \in \mathbb{R} \setminus \{0\}\} \cup \{(0,y) : y \in \mathbb{R} \setminus \{0\}\}.$$

However, this set does not contain any open subsets in $\mathbb{R}^2$. This contradicts the claimed existence of the set U, and thus proves that F is non-degenerate. □

Since the proof of the claim is complete, so is the proof of Lemma 7. □

Observe that the condition in Lemma 7 that diagonal elements are excluded from G is necessary. Indeed, in the extreme case whereby $G = \{(a,a) : a \in A\}$, we would have

$$A -_G A = A^2 -_G A^2 = A^3 -_G A^3 = \{0\}$$

and so the conclusion (9) fails in the strongest possible sense.

We will repeatedly apply a basic squeezing argument that was the key building block for the results in [8]. For convenience, we consolidate a form of it here in the following lemma.

Lemma 9. *Let $A \subset \mathbb{R}$ and write $A = \{a_1 < a_2 < \cdots < a_n\}$. Let D denote the set*

$$D := \{a_{i+1} - a_i : 1 \leqslant i \leqslant n-1\}$$

of consecutive differences determined by A. Suppose that there exists a set $D' \subset D$ and a constant L such that, for all $d \in D'$,

$$|\{i \in [n-1] \colon a_{i+1} - a_i = d\}| \geqslant L.$$

Then

$$|A + A - A| \gg |D'|^2 L.$$

Proof. Label the elements of D' in ascending order, so $D' = \{d_1 < d_2 < \dots d_t\}$, where $t = |D'|$. Fix $1 \leqslant j \leqslant t$. Since d_j has at least L representations as a consecutive difference, we may consider L distinct and disjoint intervals $(a_i, a_{i+1}]$, each with length d_j. Then, for all $1 \leqslant k \leqslant j$, we have

$$a_i < a_i + d_k \leqslant a_{i+1}.$$

Since $a_i + d_k \in A + A - A$, it follows that there are at least j elements of $A + A - A$ in the half-open interval $(a_i, a_{i+1}]$. Repeating this for each of the L choices for i, we see that this j gives rise to at least jL elements of $A + A - A$. Summing over all j, it follows that

$$|A + A - A| \geqslant \sum_{j=1}^{t} jL \gg t^2 L = |D'|^2 L. \qquad \square$$

We are now ready to prove Theorem 2.

Proof of Theorem 2. Let $N = |A|$ and label the elements of A in increasing order:

$$A = \{a_1 < a_2 < \cdots < a_N\}.$$

Consider the set

$$D := \{a_{i+1} - a_i : 1 \leqslant i \leqslant N-1\}$$

of neighboring differences of elements of A. For each $d \in D$ we define

$$r(d) = |\{1 \leqslant i \leqslant N-1 : a_{i+1} - a_i = d\}|.$$

Note that

$$\sum_{d\in D} r(d) = N - 1. \tag{15}$$

We can use a dyadic pigeonholing argument to show that there is some subset $D_1 \subset D$ and some integer L_1 such that

$$|D_1|L_1 \gtrsim N \quad \text{and} \quad \forall d \in D_1,\ L_1 < r(d) \leqslant 2L_1.$$

Since the dyadic pigeonholing technique is repeatedly used throughout this paper, we will give the full details of its first application below, and will be more succinct later. Indeed, it follows from (15) that

$$N - 1 = \sum_{d\in D} r(d) = \sum_{j=0}^{\lceil \log N \rceil} \sum_{d\in D : 2^{j-1} < r(d) \leqslant 2^j} r(d)$$

and so there exists some $0 \leqslant j_0 \leqslant \lceil \log n \rceil$ such that

$$\sum_{d\in D : 2^{j_0-1} < r(d) \leqslant 2^{j_0}} r(d) \gtrsim N.$$

Now set

$$L_1 := 2^{j_0-1} \quad \text{and} \quad D_1 := \{d \in D : L_1 < r(d) \leqslant 2L_1\}.$$

Define $H \subset A \times A$ as follows:

$$H := \{(a_i, a_{i+1}) : 1 \leqslant i \leqslant N-1, a_{i+1} - a_i \in D_1\}.$$

Note that $|H| = \sum\limits_{d\in D_1} r(d) \geqslant |D_1|L_1 \gtrsim N$. Lemma 9 implies that

$$|A + A - A| \gg |D_1|^2 L_1 \gtrsim |D_1|N = |A -_H A|N. \tag{16}$$

Now consider the set

$$A^2 -_H A^2 = \{a_{i+1}^2 - a_i^2 : (a_i, a_{i+1}) \in H\}.$$

For $d \in A^2 -_H A^2$, define

$$s(d) = |\{(a_i, a_{i+1}) \in H : a_{i+1}^2 - a_i^2 = d\}.$$

Note that $\sum_{d\in A^2 -_H A^2} s(d) = |H| \gtrsim N$. After dyadic pigeonholing again, we obtain a subset $D_2 \subset A^2 -_H A^2$ and some integer L_2 such that

$$|D_2|L_2 \gtrsim N \quad \text{and} \quad \forall d \in D_2,\ L_2 < s(d) \leqslant 2L_2.$$

Define $H' \subset H$ as follows:

$$H' := \{(a_i, a_{i+1}) \in H : a_{i+1}^2 - a_i^2 \in D_2\}.$$

Note that $|H'| = \sum_{d \in D_2} s(d) \geqslant |D_2|L_2 \gtrsim N$. Lemma 9 implies that

$$|A^2 + A^2 - A^2| \gg |D_2|^2 L_2 \gtrsim |D_2|N = |A^2 -_{H'} A^2|N. \tag{17}$$

We repeat this argument one more time. For each $d \in A^3 -_{H'} A^3$, define

$$t(d) := |\{(a_i, a_{i+1}) \in H' : a_{i+1}^3 - a_i^3 = d\}|.$$

We have $\sum_{d \in A^3 -_{H'} A^3} t(d) = |H'| \gtrsim N$. Therefore, by a further dyadic pigeonholing step, there exists $D_3 \subset A^3 -_{H'} A^3$ and some integer L_3 such that

$$|D_3|L_3 \gtrsim N \quad \text{and} \quad \forall d \in D_3,\ L_3 < t(d) \leqslant 2L_3.$$

Define $H'' \subset H' \subset H$ as follows:

$$H'' := \{(a_i, a_{i+1}) \in H' : a_{i+1}^3 - a_i^3 \in D_3\}.$$

Note that $|H''| = \sum_{d \in D_3} t(d) \geqslant |D_3|L_3 \gtrsim N$. Lemma 9 yields

$$|A^3 + A^3 - A^3| \gg |D_3|^2 L_3 \gtrsim |D_3|N = |A^3 -_{H''} A^3|N. \tag{18}$$

Now apply Lemma 7 to the set H''. We have

$$\begin{aligned}\max\{|A -_H A|, |A^2 -_{H'} A^2|, |A^3 -_{H''} A^3|\} &\geqslant \max\{|A -_{H''} A|, |A^2 -_{H''} A^2|, |A^3 -_{H''} A^3|\} \\ &\gg |H''|^{7/12} \gtrsim N^{7/12},\end{aligned}$$

where the first inequality uses the inclusions $H'' \subset H' \subset H$.

However, it then follows from (16), (17) and (18) that

$$\begin{aligned}&\max\{|A + A - A|, |A^2 + A^2 - A^2|, |A^3 + A^3 - A^3|\} \\ &\gtrsim N \cdot \max\{|A -_H A|, |A^2 -_{H'} A^2|, |A^3 -_{H''} A^3|\} \\ &\gtrsim N^{19/12},\end{aligned}$$

as required. □

3.1 Possible Generalizations of Theorem 2

Theorem 2 and its proof suggests a possible generalization, which is that the bound

$$\max\{|A + A - A|, |f(A) + f(A) - f(A)|, |g(A) + g(A) - g(A)|\} \gtrsim |A|^{19/12} \tag{19}$$

holds for suitable choices of the functions f and g. Theorem 2 proves (19) for the case $f(x) = x^2$ and $g(x) = x^3$. We have also verified that our proof works for the case when $f(x) = x^2$ and $g(x) = x^n$ for all $n \geqslant 3$. Indeed, for fixed $n \geqslant 3$, we can replace (12) with the analogous equation $e = a^n - b^n$. The resulting polynomial equation $F(x, y, z) = 0$ gives us the corresponding rational function

$$\frac{(x^2 + y)^n - (y - x^2)^n}{2x}.$$

Computing the derivative (6) gives us a more complicated, but nevertheless rational function in x and y, namely:

$$\frac{\begin{aligned}&(x^2+y)^5(x^2-y)^{4n+1} - \left(x^2-y\right)^5(x^2+y)^{4n+1} - 8(n-1)x^2y(y^2-x^4)^{2n+1}(x^4-3y^2)\\ &-2(y-x^2)^{3n}(x^2+y)^{n+3}\left((2n-3)x^6+(4n^2-12n+9)x^4y+(6n-5)x^2y^2-y^3\right)\\ &-2(y-x^2)^{n+3}(x^2+y)^{3n}\left((2n-3)x^6-(4n^2-12n+9)x^4y+(6n-5)x^2y^2-y^3\right)\end{aligned}}{(x^4-y^2)\left(2y\left(x^4-y^2\right)^{2n+1} - \left(x^2-y\right)^3\cdot\left(y+x^2\right)^{2n} + \left(x^2+y\right)^3\left(y-x^2\right)^{2n}\right)^2},$$

from which we can assert that its zero set forms a set of dimension less than or equal 1. We can therefore deduce that such a zero set does not contain any open subsets in $\mathbb{R}^2$, as needed. We expect that this setup could potentially prove (19) for the case when f and g are polynomials with distinct degrees both greater than or equal to 2, although we do not pursue this here due to the fact that the elimination method produces a polynomial of very high degree (in all variables) for F and therefore significantly increases the computational complexity of the second derivative (6).

The squeezing technique was recently used by the first author [16] to obtain growth exponent strictly greater than 3/2 with only two sets involved. More precisely, it was proven in [16] that

$$\max\{|8A - 7A|, |5f(A) - 4f(A)|\} \gg |A|^{\frac{3}{2}+\frac{1}{54}}$$

provided that f is a convex function that satisfies an additional technical condition. One can use Plünnecke's Theorem to reduce the number of variables, obtaining

$$\max\{|3A - A|, |3f(A) - f(A)|\} \gg |A|^{\frac{3}{2}+c}. \tag{20}$$

The function $f(x) = x^3$ satisfies this condition, and so (20) may be regarded as an improvement to Theorem 2. Interestingly, the case when $f(x) = x^2$ is not covered by the result in [16], and the task of proving that

$$\max\{|k_1A - k_2A|, |\ell_1A^2 - \ell_2A^2|\} \gg |A|^{\frac{3}{2}+c},$$

for some constants $k_1, k_2, \ell_1, \ell_2 \in \mathbb{N}$ and $c > 0$, remains open.

4 Proof of Theorem 1

This proof is based on the same elementary ideas that were used in [9]. However, we give a slightly different presentation of the basic idea here, which we hope is a little easier to digest. The idea of using triples was communicated to us by Misha Rudnev, who found this alternative approach to the proof of the main expander result in [9]. We are very grateful to him for sharing his ideas with us.

A two-fold squeezing argument will be used repeatedly in the proof of Theorem 11. To limit repetition, we consolidate these applications in the form of the following lemma.

Lemma 10. *Suppose that $Y = \{y_1 < y_2 < \cdots < y_n\}$ and $Z = \{z_1 < z_2 < \cdots < z_n\}$ are sets of real numbers satisfying the property that*

$$y_i < z_i \text{ for all } i \in [n] \text{ and } z_i < y_j \text{ for all } i < j.$$

In other words, the ordered set $Y \cup Z$ starts with an element of Y and then alternates between Y and Z. Write $x_i = z_i - y_i$. Suppose also that

$$x_i < x_j \text{ for all } i < j.$$

Let $I \subset [\lfloor n/2 \rfloor - 1]$ be an indexing set of integers. Then there exists a subset $I' \subset I$ such that $|I'| \gtrsim |I|$ and

$$|2Y + 2Z - 2Y - Z| \gg n^2 |\{x_{j+1} - x_j : j \in I'\}|. \tag{21}$$

Proof. Define

$$\gamma_j := x_{j+1} - x_j,$$

and

$$\Gamma := \{\gamma_j : j \leqslant \lfloor n/2 \rfloor - 1\}.$$

It is possible that $\gamma_j = \gamma_{j'}$ and $j \neq j'$. We will need to consider these potential multiplicities, and therefore define

$$r(\gamma) = |\{j \in [\lfloor n/2 \rfloor - 1] : \gamma_j = \gamma\}|.$$

Observe that

$$\sum_{\gamma \in \Gamma} r(\gamma) = \lfloor n/2 \rfloor - 1 \gg n.$$

Therefore, it follows from dyadic pigeonholing that there exists an integer L and a subset $\Gamma' \subset \Gamma$ such that

$$L \leqslant r(\gamma) < 2L, \quad \forall \gamma \in \Gamma'$$

and

$$n \lesssim |\Gamma'| L \leqslant n. \tag{22}$$

Now define $I' \subset [\lfloor n/2 \rfloor - 1]$ to be the set

$$I' := \{j : \gamma_j \in \Gamma'\}.$$

To put this another way, we have

$$\Gamma' = \{\gamma_j : j \in I'\}.$$

Observe that $|I'| \gtrsim n$. Note that this set Γ' is the set which features in the inequality (21), which we are trying to prove. In other words, our goal is to prove that

$$|2Y + 2Z - 2Y - Z| \gg n^2|\Gamma'|. \tag{23}$$

We will consider elements in $2Y + 2Z - 2Y - Z$ of the form

$$y_k + x_j + \gamma_\ell \tag{24}$$

such that

$$n/2 < k \leqslant n-1,\ j, \ell \in I',\ \gamma_\ell < \gamma_j. \tag{25}$$

It follows, from the assumption that $\gamma_\ell < \gamma_j$, that $x_j + \gamma_\ell < x_{j+1}$. Moreover, we have

$$x_j < x_j + \gamma_\ell < x_j + \gamma_j = x_j + (x_{j+1} - x_j) = x_{j+1}. \tag{26}$$

Also, since $k > n/2 > j+1$, it follows that

$$y_k < y_k + x_j + \gamma_\ell < y_k + x_{j+1} < z_k. \tag{27}$$

The last inequality is a re-writing of the bound $x_{j+1} < x_k$, which follows from the monotonicity of the x_j and the fact that $j+1 < k$.

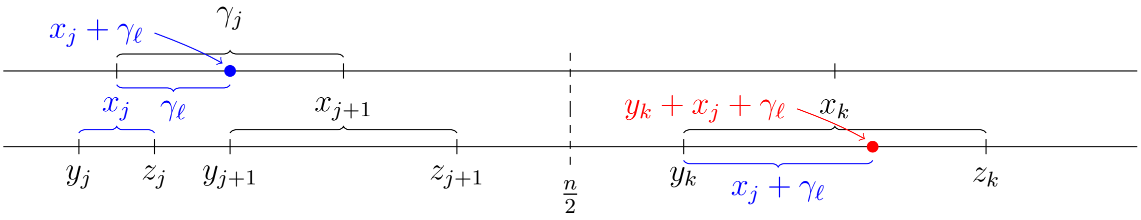

Figure 1: This figure provides a pictorial view of the "squeezing" inequalities in (26) and (27). The blue and red dots are the objects to be counted.

These inequalities allow us to squeeze sums into gaps efficiently. Indeed, let us consider a fixed k in the range given by (25). Then the sums of the form (24) belong to the interval (y_k, z_k). As k varies, these intervals are disjoint. Therefore, since the sums of the form (24) are all elements of the set $2Y + 2Z - 2Y - Z$, we have

$$\begin{aligned} 2Y + 2Z - 2Y - Z &\supseteq \{y_k + x_j + \gamma_\ell : \frac{n}{2} < k \leqslant n-1, j, \ell \in I', \gamma_\ell < \gamma_j\} \\ &= \bigcup_{\frac{n}{2} < k \leqslant n-1} \{y_k + x_j + \gamma_\ell : j, \ell \in I', \gamma_\ell < \gamma_j\}. \end{aligned}$$

This is a disjoint union, and so it follows that

$$\begin{aligned} &|2Y + 2Z - 2Y - Z| \\ &\geqslant \sum_{n/2 < k \leqslant n-1} |\{x_j + \gamma_\ell : j, \ell \in I', \gamma_\ell < \gamma_j\}| \gg n|\{x_j + \gamma_\ell : j, \ell \in I', \gamma_\ell < \gamma_j\}|. \end{aligned} \tag{28}$$

Moreover, we can use a second squeeze, coming from (26), to obtain a lower bound for the size of the set $\{x_j + \gamma_\ell : j, \ell \in I', \gamma_\ell < \gamma_j\}$. For fixed $j \in I'$, it follows from (26) that

$$x_j + \gamma_\ell \in (x_j, x_{j+1})$$

for all ℓ such that $\gamma_\ell < \gamma_j$. As j varies, these intervals are disjoint. Therefore,

$$|\{x_j + \gamma_\ell : j, \ell \in I', \gamma_\ell < \gamma_j\}| = \sum_{j \in I'} |\{\ell \in I' : \gamma_\ell < \gamma_j\}|. \tag{29}$$

This sum can be seen as the sum over all $j \in I'$ of the rank of j, where the rank of j tells us the position of γ_j in the ordered set Γ'. By the dyadic pigeonholing argument used to construct the set Γ', at most $2L$ elements j can have the same rank. Therefore, (29) is a sum of $|I'|$ non-negative integers, each occuring with multiplicity in between L and $2L$. Since $|I'| \gtrsim n$, it follows that for some absolute constant c,

$$|\{x_j + \gamma_\ell : j, \ell \in I_1, \gamma_\ell < \gamma_j\}| \geqslant L \sum_{j=0}^{cn/(L \log n)} j \gtrsim \frac{n^2}{L} \geqslant n|\Gamma'|.$$

We have used the upper bound in (22) for the last inequality. It therefore follows from (28) that

$$|2Y + 2Z - 2Y - Z| \gg n^2 |\Gamma'|.$$

This proves (23), and therefore completes the proof of the lemma. □

Next, we restate Theorem 1 in a way that makes for more convenient generalization.

Theorem 11. *Let $A \subset \mathbb{R}$ and define the function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \ln(e^x + 1)$. Then there exist $a, a' \in A$ such that*

$$|2f(a + A) + 2f(a' + A) - 2f(a + A) - f(a' + A)| \gtrsim |A|^{31/12}.$$

Let us quickly verify that this result does imply Theorem 1. Note that there exists a subset $X' \subset X$ with $|X'| \geqslant |X|/2 - 1$ such that all of the elements of X' have the same sign. If all of the elements of X' are positive then apply Theorem 11, taking $A = \ln X'$. Otherwise, all of the elements of X' are negative and we can apply Theorem 11 with $A = \ln(-X')$. It remains to prove Theorem 11.

Proof of Theorem 11. Label the elements of A in ascending order, so $A = \{a_1 < \cdots < a_n\}$. Identify two "nextdoor but two" elements of A which are closest. That is, let a_i and a_{i+3} be two elements of A such that

$$a_{i+3} - a_i = \min\{a_{j+3} - a_j : 1 \leqslant j \leqslant n - 3\}. \tag{30}$$

Then, for every third element a_{3j} of A, where $1 \leqslant j \leqslant \lfloor n/3 \rfloor$, we consider the interval

$$(a_i + a_{3j}, a_{i+3} + a_{3j}).$$

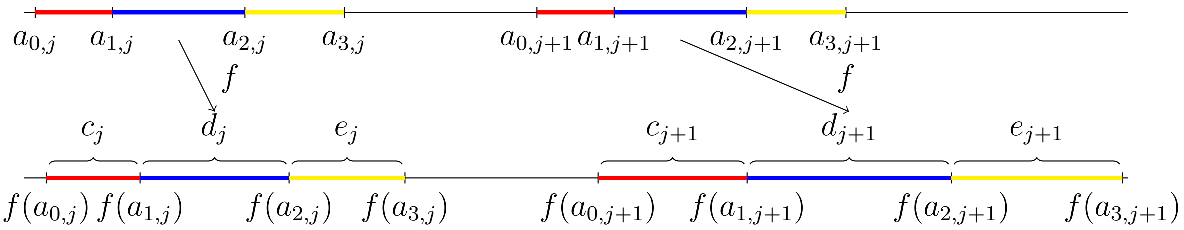

Figure 2: This figure illustrates the setup for the proof of Theorem 11. In the proof, we begin by finding many identical intervals, divided into three parts (color-coded in the figure for convenience), with endpoints in $A + A$ which do not overlap. This is illustrated in the top line. Application of our strictly convex function f to these intervals changes their lengths. This is illustrated in the second line. After the application, the lengths of the colored intervals form an increasing sequence as j increases. This puts us in a situation where we can look to apply Lemma 10 for each of these sets of increasing intervals.

Note that all of these intervals have the same length, which is $a_{i+3} - a_i$. Moreover, as j varies, these intervals are disjoint. Indeed, suppose that two neighboring such intervals

$$(a_i + a_{3j}, a_{i+3} + a_{3j}) \text{ and } (a_i + a_{3(j+1)}, a_{i+3} + a_{3(j+1)})$$

overlap. Then it follows that

$$a_i + a_{3(j+1)} < a_{i+3} + a_{3j}.$$

This rearranges to give

$$a_{3j+3} - a_{3j} < a_{i+3} - a_i,$$

which contradicts the minimality of $a_{i+3} - a_i$ established in (30).

We now apply the function f to these intervals, so that we consider the intervals

$$(f(a_i + a_{3j}), f(a_{i+3} + a_{3j})) \text{ such that } 1 \leqslant j \leqslant \lfloor n/3 \rfloor. \tag{31}$$

Note that f is strictly convex. It therefore follows that the intervals considered in (31) have lengths which are strictly increasing as j increases.

We will make use of three applications of Lemma 10. To this end, we define

$$\begin{aligned} c_j &:= f(a_{i+1} + a_{3j}) - f(a_i + a_{3j}), \\ d_j &:= f(a_{i+2} + a_{3j}) - f(a_{i+1} + a_{3j}), \\ e_j &:= f(a_{i+3} + a_{3j}) - f(a_{i+2} + a_{3j}). \end{aligned}$$

See Figure 2 for a visual explanation of the sequences for these intervals $\{c_j\}_{j\geqslant1}$, $\{d_j\}_{j\geqslant1}$, and $\{e_j\}_{j\geqslant1}$. In Figure 2, for the purposes of making the annotations readable, we use $a_{k,j}$ as a temporary shorthand to represent $a_{i+k} + a_{3j}$.

In words, c_j is the difference between the first and second points of the j'th interval identified in (31), d_j is the difference between the second and third points of the j'th interval, and e_j is the difference between the third and fourth points of the j'th interval. Since f is strictly convex, each of these quantities are strictly increasing with j. That is, we have

$$c_j < c_{j+1},\ d_j < d_{j+1},\ e_j < e_{j+1}$$

for all $1 \leqslant j \leqslant \lfloor n/3 \rfloor - 1$.

Apply Lemma 10 with

$$Y = \{f(a_i + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\}, \quad Z = \{f(a_{i+1} + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\},$$

$$x_j = c_j, \quad \text{and} \quad I = [\lfloor n/6 \rfloor - 1].$$

It follows that there exists $I_1 \subset [\lfloor n/6 \rfloor - 1]$ such that

$$|I_1| \gtrsim n$$

and

$$|2f(a_i + A) + 2f(a_{i+1} + A) - 2f(a_i + A) - f(a_{i+1} + A)| \gg n^2 |\{c_{j+1} - c_j : j \in I_1\}|. \quad (32)$$

Next, we make a second application of Lemma 10. This time, we set

$$Y = \{f(a_{i+1} + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\}, \quad Z = \{f(a_{i+2} + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\},$$

$$x_j = d_j, \quad \text{and} \quad I = I_1.$$

It follows that there exists $I_2 \subset I_1$ such that

$$|I_2| \gtrsim |I_1| \gtrsim n$$

and

$$|2f(a_{i+1} + A) + 2f(a_{i+2} + A) - 2f(a_{i+1} + A) - f(a_{i+2} + A)| \gg n^2 |\{d_{j+1} - d_j : j \in I_2\}|. \quad (33)$$

For the third application of Lemma 10, set

$$Y = \{f(a_{i+2} + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\}, \quad Z = \{f(a_{i+3} + a_{3j}) : 1 \leqslant j \leqslant \lfloor n/3 \rfloor\},$$

$$x_j = e_j, \quad \text{and} \quad I = I_2.$$

It follows that there exists $I_3 \subset I_2 \subset I_1$ such that

$$|I_3| \gtrsim |I_2| \gtrsim n$$

and

$$|2f(a_{i+2} + A) + 2f(a_{i+3} + A) - 2f(a_{i+2} + A) - f(a_{i+3} + A)| \gg n^2 |\{e_{j+1} - e_j : j \in I_3\}|. \quad (34)$$

Next, define

$$\Gamma := \{c_{j+1} - c_j : j \in I_3\}, \quad \Delta := \{d_{j+1} - d_j : j \in I_3\}, \ \ \mathcal{E} := \{e_{j+1} - e_j : j \in I_3\}.$$

It now follows from (32), (33) and (34), along with the inclusions $I_3 \subset I_2 \subset I_1$ that there exist $a, a' \in A$ such that

$$|2f(a+A) + 2f(a'+A) - 2f(a+A) - f(a'+A)| \gtrsim n^2 \max\{|\Gamma|, |\Delta|, |\mathcal{E}|\}. \tag{35}$$

The last task is for us to prove the following claim.

Claim 12.

$$\max\{|\Gamma|, |\Delta|, |\mathcal{E}|\} \gg n^{7/12}.$$

Once this claim is proven, the proof of the theorem will follow from (35). It remains to prove the claim.

Proof of Claim. We will double count solutions to the system of equations

$$\begin{aligned} \gamma &= c_{j+1} - c_j, \\ \delta &= d_{j+1} - d_j, \\ \varepsilon &= e_{j+1} - e_j, \end{aligned} \tag{36}$$

such that

$$\gamma \in \Gamma, \ \delta \in \Delta, \ \varepsilon \in \mathcal{E}, \ j \in I_3.$$

Let S denote the number of solutions to this system. We note here that we do not get any solutions to this system with any of γ, δ or ε equal to 0. Indeed, this follows from our knowledge that $c_{j+1} > c_j$, $d_{j+1} > d_j$ and $e_{j+1} > e_j$.

The easy task is to give a lower bound. Indeed, since each $j \in I_3$ gives a contribution to S, we have

$$S = |I_3| \gtrsim n. \tag{37}$$

To obtain an upper bound for S, we will unravel the definitions which are used in (36). We remark here that, until this point, we have not used the specified information that $f(x) = \ell\text{n}(e^x + 1)$. The only property of this function that we have used is that f is strictly convex.

Plugging the definitions of c_j, d_j and e_j into (36), we can rewrite it in the form

$$\begin{aligned} \gamma &= f(a_{i+1} + a_{3(j+1)}) - f(a_i + a_{3(j+1)}) - f(a_{i+1} + a_{3j}) + f(a_i + a_{3j}), \\ \delta &= f(a_{i+2} + a_{3(j+1)}) - f(a_{i+1} + a_{3(j+1)}) - f(a_{i+2} + a_{3j}) + f(a_{i+1} + a_{3j}), \\ \varepsilon &= f(a_{i+3} + a_{3(j+1)}) - f(a_{i+2} + a_{3(j+1)}) - f(a_{i+3} + a_{3j}) + f(a_{i+2} + a_{3j}). \end{aligned} \tag{38}$$

Recall that the elements a_i, a_{i+1}, a_{i+2} and a_{i+3} are not variables here. They were fixed at the beginning of the proof when we chose close near-neighbors a_i and a_{i+3}. Write

$a_k = \ell\mathrm{n}(s_k)$ for all $1 \leqslant k \leqslant n$. We can finally use the information that $f(x) = \ell\mathrm{n}(e^x + 1)$ to rewrite this system once again. After some rearranging, we obtain

$$\begin{aligned} e^{\gamma} &= \frac{(s_{i+1}s_{3(j+1)} + 1)(s_i s_{3j} + 1)}{(s_i s_{3(j+1)} + 1)(s_{i+1}s_{3j} + 1)}, \\ e^{\delta} &= \frac{(s_{i+2}s_{3(j+1)} + 1)(s_{i+1}s_{3j} + 1)}{(s_{i+1}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1)}, \\ e^{\varepsilon} &= \frac{(s_{i+3}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1)}{(s_{i+2}s_{3(j+1)} + 1)(s_{i+3}s_{3j} + 1)}. \end{aligned} \tag{39}$$

After relabeling the variables, we seek an upper bound for the number of solutions to the system

$$\begin{aligned} \overline{x} &= \frac{(s_{i+1}s_{3(j+1)} + 1)(s_i s_{3j} + 1)}{(s_i s_{3(j+1)} + 1)(s_{i+1}s_{3j} + 1)}, \\ \overline{y} &= \frac{(s_{i+2}s_{3(j+1)} + 1)(s_{i+1}s_{3j} + 1)}{(s_{i+1}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1)}, \\ \overline{z} &= \frac{(s_{i+3}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1)}{(s_{i+2}s_{3(j+1)} + 1)(s_{i+3}s_{3j} + 1)}, \end{aligned} \tag{40}$$

such that

$$\overline{x} \in e^{\Gamma},\ \overline{y} \in e^{\Delta},\ \overline{z} \in e^{\mathcal{E}},\ j \in I_3.$$

Since we do not have any solutions to (36) with any of $\gamma, \delta, \varepsilon = 0$, it follows that there are no solutions to (40) with any of $\overline{x}, \overline{y}$ or $\overline{z}$ equal to 1.

For the goal of finding an upper bound to the number of solutions to (40), we use the Elekes-Szabó Theorem in much the same way as the proof of Lemma 7. We first use Singular's Eliminate [4, 10] to compute the elimination ideal generated by the polynomials

$$\begin{gathered} (s_i s_{3(j+1)} + 1)(s_{i+1}s_{3j} + 1)x - (s_{i+1}s_{3(j+1)} + 1)(s_i s_j + 1), \\ (s_{i+1}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1)y - (s_{i+1}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1), \\ (s_{i+2}s_{3(j+1)} + 1)(s_{i+3}s_{3j} + 1)z - (s_{i+3}s_{3(j+1)} + 1)(s_{i+2}s_{3j} + 1), \end{gathered}$$

which eliminates s_{3j} and $s_{3(j+1)}$ from this system and reduces it to a single polynomial in three variables x, y and z. From there, we deduce that every contribution (x, y, z, j) to S gives rise to a solution to the polynomial equation $F(x, y, z) = 0$, where

$$F(x, y, z) := (x-1)(z-1) \cdot G(x, y, z), \tag{41}$$

with G defined to be

$$\begin{aligned} G(x, y, z) := &(xy^2z + 1)(s_i - s_{i+1})(s_{i+2} - s_{i+3}) \\ &+ (xyz + y)(s_{i+2} - s_i)(s_{i+1} - s_{i+3}) \\ &+ (yz + xy)(s_i - s_{i+3})(s_{i+1} - s_{i+2}). \end{aligned}$$

Since there are no contributions to S with $x = 1$ or $z = 1$, it follows that every contribution (x, y, z, j) to S gives rise to a solution to the polynomial equation $G(x, y, z) = 0$. Therefore, we have

$$S \leqslant |Z(G) \cap (e^{\Gamma} \times e^{\Delta} \times e^{\mathcal{E}})|. \tag{42}$$

Note that all of the coefficients in G are non-zero, since $s_i < s_{i+1} < s_{i+2} < s_{i+3}$. We now proceed to verify that G is non-degenerate. In order to see this, we note that z can be expressed as a rational function of x and y, i.e.,

$$z = \frac{-xy(s_i - s_{i+3})(s_{i+1} - s_{i+2}) - y(s_{i+2} - s_i)(s_{i+1} - s_{i+3}) - (s_i - s_{i+1})(s_{i+2} - s_{i+3})}{xy^2(s_i - s_{i+1})(s_{i+2} - s_{i+3}) + xy(s_{i+2} - s_i)(s_{i+1} - s_{i+3}) + y(s_i - s_{i+3})(s_{i+1} - s_{i+2})}.$$

Denote the right hand side of this expression to be $g(x, y)$ (note that this is $f(x, y)$ from Lemma 5 but we changed the name to distinguish it from the f in this proof). Then the computation of

$$\frac{\partial^2(\ell\text{n}\, |g_x/g_y|)}{\partial x \partial y}$$

turns out to be the rational function

$$\frac{\begin{array}{l} -2 \cdot \big(\left(x^2y^2 + 1\right) \left(s_i - s_{i+1}\right) \left(s_{i+1} - s_{i+2}\right) \left(s_i - s_{i+3}\right) \\ \qquad + \left(x^2y + y\right) \left(s_i - s_{i+2}\right) \left(s_{i+1} - s_{i+2}\right) \left(s_i - s_{i+3}\right) \left(s_{i+1} - s_{i+3}\right) \\ \qquad + \left(2xy\right) \left(s_{i+1} - s_{i+2}\right)^2 \left(s_i - s_{i+3}\right)^2 \big) \end{array}}{\begin{array}{l} \big((x^2y^2 + 1)(s_{i+1} - s_{i+2})(s_i - s_{i+3}) - (xy^2 + x)(s_i - s_{i+2})(s_{i+1} - s_{i+3}) \\ \quad + (2xy)(s_i - s_{i+1})(s_{i+2} - s_{i+3}) - x(s_i - s_{i+2})(s_{i+1} - s_{i+3}) \big)^2 \end{array}}, \tag{43}$$

which is an expression that is zero when

$$y = \begin{cases} r_1 \pm \frac{1}{2}\sqrt{r_2}, & x \neq 0, \\ \dfrac{(s_i - s_{i+1})(s_{i+2} - s_{i+3})}{(s_i - s_{i+2})(s_{i+1} - s_{i+3})}, & x = 0, \end{cases} \tag{44}$$

with

$$r_1 := \frac{\left(x^2 + 1\right) \left(s_i - s_{i+2}\right) \left(s_{i+1} - s_{i+3}\right) - 2x \left(s_{i+1} - s_{i+2}\right) \left(s_i - s_{i+3}\right)}{2x^2 \left(s_i - s_{i+1}\right) \left(s_{i+2} - s_{i+3}\right)},$$

$$r_2 := \frac{\begin{array}{c} \left(x^2 + 1\right) \left(s_i s_{i+1} - s_{i+2} s_{i+1} + s_{i+2} s_{i+3}\right)\left(s_i s_{i+1} - s_{i+2} s_{i+1} - 2 s_i s_{i+3} + s_{i+2} s_{i+3}\right) \\ -2x \left(s_i - s_{i+2}\right)\left(s_{i+1} - s_{i+3}\right)\left(s_i s_{i+1} + s_{i+2} s_{i+1} - 2 s_{i+3} s_{i+1} - 2 s_i s_{i+2} + s_i s_{i+3} + s_{i+2} s_{i+3}\right) \end{array}}{x^4 \left(s_i - s_{i+1}\right)^2 \left(s_{i+2} - s_{i+3}\right)^2}.$$

The pairs (x, y) that satisfy (44) form a set of measure zero in $\mathbb{R}^2$. Hence, there are no open subsets in $\mathbb{R}^2$ for which (43) is identically zero. By Lemma 5, we can conclude that G is non-degenerate.

Since G is non-degenerate, it follows from Theorem 3 that

$$|Z(G) \cap (e^{\Gamma} \times e^{\Delta} \times e^{\mathcal{E}})| \ll \max\{|\Gamma|, |\Delta|, |\mathcal{E}|\}^{12/7}.$$

Combining this with (42) and (37), it follows that

$$\max\{|\Gamma|, |\Delta|, |\mathcal{E}|\} \gtrsim n^{7/12},$$

as required.

□

This completes the proof of Theorem 11. □

5 Conclusions and Future Directions

We conclude this paper by discussing a few variations of Theorem 11, in which we make different choices for the function f. We observe that most of the proof uses only the fact that f is a strictly convex function. However, we eventually need to know something more concrete about f in order to calculate F in the form of (41), and to check whether or not it is degenerate.

Firstly, we note that we can repeat the proof of Theorem 11 with minimal changes for the case when $f(x) = \ell\mathrm{n}(e^x + \lambda)$ and λ is a strictly positive real number. That is, we have the following theorem.

Theorem 13. *Let $A \subset \mathbb{R}$ and let $\lambda > 0$ be a real number. Define the function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \ell\mathrm{n}(e^x + \lambda)$. Then there exist $a, a' \in A$ such that*

$$|2f(a + A) + 2f(a' + A) - 2f(a + A) - f(a' + A)| \gtrsim |A|^{31/12}.$$

This in turn implies an analog of Theorem 1: for any $X \subset \mathbb{R}$ and any $\lambda > 0$, there exist $x, x' \in X$ such that

$$\left| \frac{(xX + \lambda)^{(2)}(x'X + \lambda)^{(2)}}{(xX + \lambda)^{(2)}(x'X + \lambda)} \right| \gtrsim |X|^{31/12}.$$

We can also prove a similar result for $\lambda < 0$, although a little more care is needed to ensure we are not attempting to take logarithms of negative values.

We attempted to prove a version of Theorem 11 with $f(x) = x^3$ and $f(x) = x^4$. For the case $f(x) = x^3$, we discovered that the corresponding polynomial $F(x, y, z)$ is linear in each of the three variables and thus degenerate, so Theorem 3 could not be applied. For the case when $f(x) = x^4$, we calculated that the corresponding polynomial $F(x, y, z)$ is quartic in all 3 variables, and we were not able to verify that this polynomial is non-degenerate using Lemma 6 as (6) turned out to be too computationally complex. Nevertheless, we expect that such results for $f(x) = x^n$ with $n \geqslant 3$ are true.

These cases illustrate a general problem with the method: on one hand, we have a useful derivative test in the form of Lemma 6 to check whether a given polynomial $F(x, y, z)$

satisfies the non-degeneracy conditions of Theorem 3. On the other hand, when it either gets too computationally complex (as it often does) or we get no useful information because the second derivative is identically zero, the use of alternative strategies tend to be more ad-hoc and adapted according to the underlying geometric properties of the problem at-hand. Thus, a reasonable direction of research could be to identify another systematic way in which we could determine non-degeneracy of polynomials in the sense of Definition 4 for the purpose of taking advantage of the result of Elekes and Szabó.

Acknowledgements

O. Roche-Newton was supported by the Austrian Science Fund FWF Project P34180. E. Wong was mostly supported by the Austrian Academy of Sciences at the Radon Institute for Computational and Applied Mathematics (RICAM) during the writing and preparation of this article. We are grateful to Orit Raz and Audie Warren for helpful input when putting together this paper.

References

[1] P. J. Bradshaw. Growth in Sumsets of Higher Convex Functions. *Combinatorica* 43, 769–789 (2023). https://doi.org/10.1007/s00493-023-00035-6

[2] P. J. Bradshaw, B. Hanson, and M. Rudnev. Higher Convexity and Iterated Second Moment Estimates. *The Electronic Journal of Combinatorics*, 29(3) (2021). #P3.6 https://doi.org/10.37236/10773

[3] F. de Zeeuw. A Survey of Elekes–Rónyai-Type Problems. In: Ambrus, G., Bárány, I., Böröczky, K., Fejes Tóth, G., Pach, J. (eds). *New Trends in Intuitive Geometry*, Bolyai Society Mathematical Studies 27. Springer, Berlin, Heidelberg (2018). https://doi.org/10.1007/978-3-662-57413-3_5

[4] W. Decker, G. M. Greuel, G. Gfister, and H. Schoönemann. Singular 4-1-1-3 — A Computer Algebra System for Polynomial Computations (2022). https://www.singular.uni-kl.de

[5] G. Elekes, M. Nathanson, and I. Ruzsa. Convexity and Sumsets. *Journal of Number Theory*, 83:194–201 (1999). https://doi.org/10.1006jnth.1999.2386

[6] G. Elekes and L. Rónyai. A Combinatorial Problem on Polynomials and Rational Functions. *Journal of Combinatorial Theory, Series A*, 89:1–20 (2000). https://doi.org/10.1006/jcta.1999.2976

[7] G. Elekes and E. Szabó. How to find groups? (And how to use them in Erdős geometry?). *Combinatorica*, 32(5):537–571 (2012). https://doi.org/10.1007/s00493-012-2505-6

[8] B. Hanson, O. Roche-Newton, and M. Rudnev. Higher Convexity and Iterated Sum Sets. *Combinatorica*, 42, 71–85 (2022). https://doi.org/10.1007/s00493-021-4578-6

[9] B. Hanson, O. Roche-Newton, and S. Senger. Convexity, Superquadratic Growth, and Dot Products. *Journal of the London Mathematical Society*, 107(5), 1900–1923 (2023). https://doi.org/10.1112/jlms.12728

[10] M. Kauers and V. Levandovskyy. An Interface Between Mathematica and Singular. Technical Report 2006-29, SFB F013. Johannes Kepler Universität, Linz, Austria (2006). https://www3.risc.jku.at/research/combinat/software/Singular/

[11] M. Makhul, O. Roche-Newton, S. Stevens, and A. Warren. The Elekes-Szabó Problem and the Uniformity Conjecture. *Israel Journal of Mathematics*, 248, 39–66 (2022). https://doi.org/10.1007/s11856-022-2291-9

[12] M. Makhul, O. Roche-Newton, A. Warren, and F. de Zeeuw. Constructions for the Elekes-Szabó and Elekes-Rónyai Problems. *The Electronic Journal of Combinatorics*, 27(1) (2020). #P1.57. https://doi.org/10.37236/8668

[13] M. Mudgal. Energy Estimates in Sum-Product and Convexity Problems. Preprint on arXiv (2021). https://doi.org/10.48550/arXiv.2109.04932

[14] O. E. Raz, M. Sharir, and F. de Zeeuw. Polynomials Vanishing on Cartesian Products: The Elekes-Szabó Theorem Revisited. *Duke Mathematics Journal*, 165(18):3517–3566 (2016). https://doi.org/10.1215/00127094-3674103

[15] O. E. Raz, M. Sharir, and J. Solymosi. Polynomials Vanishing on Grids: The Elekes–Rónyai Problem Revisited. *American Journal of Mathematics*, 138:1029–1065 (2016). https://doi.org/10.1353/ajm.2016.0033

[16] O. Roche-Newton. A better than 3/2 exponent for iterated sums and products over $\mathbb{R}$. Preprint on arXiv (2023). https://doi.org/10.48550/arXiv.2304.00853

[17] O. Roche-Newton. Sums, Products, and Dilates on Sparse Graphs. *SIAM Journal of Discrete Mathematics*, 35(1):194–204 (2021). https://doi.org/10.1137/20M1372184

[18] I. Z. Ruzsa, G. Shakan, J. Solymosi, and E. Szemerédi. On Distinct Consecutive Differences. In M.B. Nathanson, editor, *Combinatorial and Additive Number Theory IV (CANT)*, v.347. Springer Proceedings in Mathematics and Statistics, Cham, Switzerland (2020). https://doi.org/10.1007/978-3-030-67996-5_24

[19] I. D. Shkredov and J. Solymosi. The Uniformity Conjecture in Additive Combinatorics. *SIAM Journal of Discrete Mathematics*, 35(1):307–321, 2021. https://doi.org/10.1137/20M1367672

[20] J. Solymosi and J. Zahl. Improved Elekes-Szabó type Estimates Using Proximity. *Journal of Combinatorial Theory, Series A*. 201 (2024) 105813. https://doi.org/10.1016/j.jcta.2023.105813