On sum sets and convex functions

Sophie Stevens Audie Warren
Johann Radon Institute for Computational and Applied Mathematics
Linz, Austria
{sophie.stevens,audie.warren}@oeaw.ac.at

Submitted: Nov 4, 2021; Accepted: Feb 21, 2022; Published: May 6, 2022

Abstract

In this paper we prove new bounds for sums of convex or concave functions. Specifically, we prove that for all $A, B \subseteq \mathbb{R}$ finite sets, and for all f, g convex or concave functions, we have

$$|A+B|^{38}|f(A)+g(B)|^{38} \gtrsim |A|^{49}|B|^{49}.$$

This result can be used to obtain bounds on a number of two-variable expanders of interest, as well as to the asymmetric sum-product problem. We also adjust our technique to prove the three-variable expansion result

$$|AB+A| \gtrsim |A|^{\frac{3}{2}+\frac{3}{170}}.$$

Our methods follow a series of recent developments in the sum-product literature, presenting a unified picture. Of particular interest is an adaptation of a regularisation technique of Xue, originating in a paper of Rudnev, Shakan, and Shkredov, that enables us to find positive proportion subsets with certain desirable properties.

Mathematics Subject Classifications: 11B30, 05A20

Introduction

Given finite sets A and B of real numbers, the *sum set* and *product set* of A and B are defined as

$$A+B = \{a+b : a \in A, b \in B\}, \quad AB = \{ab : a \in A, b \in B\}.$$

Erdős and Szemerédi conjectured that at least one of $|A+A|$ or $|AA|$ is large with respect to $|A|$. Specifically, they conjectured the following.[1]

Conjecture 1 (Erdős - Szemerédi). For all $A \subseteq \mathbb{Z}$ a finite set, and for all $\epsilon > 0$, we have

$$|AA| + |A+A| \gg |A|^{2-\epsilon}.$$

This conjecture remains open, and has given rise to the study of the *sum-product* phenomenon, which, loosely defined, is the notion that finite sets cannot be simultaneously additively and multiplicatively structured. Conjecture 1 is believed to be true over the real numbers, where current progress is given by Rudnev and Stevens [13].

There are many variants of this problem in the literature; one family of such variants are concerned with convex functions[2]. Such results quantify the notion that *convex functions destroy additive structure.* Some examples of common problems in this area are the following:

For $A \subseteq \mathbb{R}$ a finite set, and f be a convex function:

- Is the set $A + f(A)$ always large?
- Is at least one of the sets $A + A$ or $f(A) + f(A)$ always large?

Much research has been done towards these problems and their variants, see for instance [2, 3, 5]. This is also related to the notion of a *convex set*, that is, a set $A = \{a_1 < a_2 < \cdots < a_n\}$ such that $a_{i+1} - a_i > a_i - a_{i-1}$ for all $2 \leqslant i \leqslant n-1$. Any convex set is the image of the interval $[n]$ under some convex function f. Current progress for these problems is given, respectively, by Li and Roche-Newton, [5] and Shkredov [17].

Theorem 2 (Li, Roche-Newton)**.** *Let $A \subseteq \mathbb{R}$ be a finite set, and let f be a convex function. Then we have*

$$|A + f(A)| \gtrsim |A|^{\frac{24}{19}}.$$

Theorem 3 (Shkredov)**.** *Let $A \subseteq \mathbb{R}$ be a finite set, and let f be a convex function. Then we have*

$$|A + A| + |f(A) + f(A)| \gtrsim |A|^{\frac{100}{79}}.$$

These problems are also related to *expander* results. Results of this nature state that some set, defined by (typically polynomial) combinations of elements of A, is *always* large. Two of the simplest examples of expanders are the sets

$$AA + A = \{ab + c : a, b, c \in A\}, \qquad A(A + 1) = \{a(b + 1) : a, b \in A\}$$

which are both expected to have size at least $|A|^{2-\epsilon}$ for all $\epsilon > 0$. In fact, the expander $A(A + 1)$ is a special case of the set $A + f(A)$ from above. The current bounds in the literature for these expanders are due to Roche-Newton and Warren [9] and Jones and Roche-Newton [4], respectively.

Theorem 4 (Roche-Newton, Warren)**.** *For all $A \subseteq \mathbb{R}$ finite, we have*

$$|AA + A| \gtrsim |A|^{\frac{3}{2} + \frac{1}{194}}.$$

Theorem 5 (Jones, Roche-Newton)**.** *For all $A \subseteq \mathbb{R}$ finite, we have*

$$|A(A + 1)| \gtrsim |A|^{\frac{24}{19}}.$$

[1] In this paper we use the standard notation $X \ll Y$ to mean that there exists an absolute constant c with $X \leqslant cY$. We have $Y \gg X$ iff $X \ll Y$. The symbols $\lesssim$ and $\gtrsim$ are used to suppress logarithmic factors, and we write $X \sim Y$ if we have $X \lesssim Y \lesssim X$.

[2] In this paper all convex functions considered are *strictly* convex functions. Furthermore, our results also apply to strictly *concave* functions.

Main Results

The proof of the sum-product result in [13] makes use of a combination of techniques used previously in the real numbers, combined with a technique used to prove sum-product results in finite fields, see [10]. In this paper we extend these techniques to give both quantitative and qualitative improvements to the problems mentioned above. Note that we make no attempt to optimise the logarithmic factors in our results, since in all cases the polynomial factor exponents are not expected to be tight. Our main result is the following.

Theorem 6. *Let $A, B \subseteq \mathbb{R}$ be finite sets, and let f and g each be either a convex or concave function. Then we have*

$$|A+B|^{38}|f(A)+g(B)|^{38} \gtrsim (|A||B|)^{49}.$$

For certain choices of A, B, f, and g, this theorem implies improvements to many of the problems mentioned above. Firstly, we can recover the following improvements to Theorems 2 and 3.

Corollary 7. *For all $A \subseteq \mathbb{R}$ finite, and f a convex function, we have*

$$|A+f(A)| \gtrsim |A|^{49/38},$$

$$|A+A| + |f(A)+f(A)| \gtrsim |A|^{49/38}.$$

The first inequality follows from setting $B = f(A)$ and $g = f^{-1}$. The second follows from setting $B = A$ and $f = g$. By slightly adjusting the proof of Theorem 6, we can obtain a better bound for differences.

Corollary 8. *For all $A \subseteq \mathbb{R}$ finite, and f a convex function, we have*

$$|A-A|^5|f(A)-f(A)|^5 \gtrsim |A|^{13}.$$

In the case $A = [1, \ldots, n]$, this matches the bounds of Schoen and Shkredov [15] and Rudnev and Stevens [13] for estimates on differences and sums of convex sets respectively. Furthermore we match the result of Li and Roche-Newton [5] in the case of few differences, many convex differences.

Secondly, we find an asymmetric sum-product result.

Corollary 9. *For all $A, B \subseteq \mathbb{R}$ finite, we have*

$$|AB|^{38}|A+B|^{38} \gtrsim (|A||B|)^{49}.$$

This follows from setting $A = X$, $B = Y$, $f = g = \log(x)$. Corollary 9 appears to be a little studied variant of the asymmetric sum-product problem: One example of a result in this direction is by Solymosi [19], who showed that $|A+A||B+B||AB| \gtrsim |A|^2|B|^2$. There has also been work towards the more difficult problem of finding a lower bound on $|A+B||AC|$, see for instance [2], or [6, Theorem 10], where the results are rather of a qualitative nature. The statement of Corollary 9 is particularly interesting in the extremal cases of 'few sums' or 'few products': e.g. if $|A| = |B| = N$ and $|A+B| \lesssim N$, then $|AB| \gtrsim N^{\frac{3}{2}+\frac{3}{38}}$. Typically the exponent of 3/2 is a barrier in sum-product estimates, and so in this sense, Corollary 9 is threshold-breaking.

Thirdly we give some results demonstrating the principle that 'translation destroys multiplicative structure', in particular improving Theorem 5.

Corollary 10. *For all $A, B \subseteq \mathbb{R}$ finite, we have*

$$|A(A+1)| \gtrsim |A|^{49/38},$$

$$|AB| + |(A+1)(B+1)| \gtrsim (|A||B|)^{49/76}.$$

Finally, by combining techniques used in the proof of Theorem 6 with the method of Roche-Newton and Warren, we can give an improvement and generalisation of Theorem 4.

Theorem 11. *Let $A, B \subseteq \mathbb{R}$ be finite sets with $|A| \sim |B|$. Then we have*

$$|AB + A| \gtrsim |A|^{\frac{3}{2}+\frac{3}{170}}.$$

Techniques

Here we give an overview of the techniques that we use, hinting at the aspects of our method that are most amenable to future improvements. These techniques can be summarised as follows:

1. The Szemerédi-Trotter theorem gives good bounds on $\mathsf{E}_3^+(A, B)$, especially if we have data of the form $r_{QR}(a) \geqslant T$ for each $a \in A$. Similarly, the Szemerédi-Trotter theorem gives good bounds on $\mathsf{E}_3^+(f(A), B)$ for a convex function f, if we have data of the form $r_{Q-R}(a) \geqslant T$ for each $a \in A$.

2. Using a regularisation result, we can find a subset $C \subseteq A$ so that $|C| \gtrsim |A|$ and for which we have the additive data $r_{Q-R}(c) \geqslant T$ for each $c \in C$.

3. We can count solutions (a, b, c) to a tautological equation of the form $a - b = (a+c) - (b+c)$, where we insist that $a - b, a + c$ are in certain (different) sets via third moment energy bounds. This gives an auxiliary energy bound, see Proposition 17 below.

4. A corollary of the regularisation result (see Corollary 16 below) allowing us to upper bound certain products of energies, together with this auxiliary energy bound, leads to the result.

Underlying many results about expander sets in $\mathbb{R}$ (with few variables) is the Szemerédi-Trotter theorem. It is common knowledge that the Szemerédi-Trotter theorem is particularly strong for finding bounds on the third moment energy $\mathsf{E}_3^+(A,B)$, an idea first introduced by Schoen and Shkredov [15]. This, in part, is due to the 'trick' that every element of A can be written as a product of elements of AA and A in at least $|A|$ ways: $a = (ab)/b$ for any choice of $b \in A$ (we assume here that $0 \notin A$). However, if one has additional multiplicative structure on A, say $r_{QR}(a) \geqslant T$ for each $a \in A$ and some auxiliary sets Q and R and a number T, one can use this information in place of the aforementioned 'trick'. This gives a third moment energy bound in terms of Q, R and T, the strength of which depends on the strength of the multiplicative information. This is the idea behind the so-called *Szemerédi-Trotter sets* introduced by Shkredov [17], for which the notation $d^+(A)$ (and variants thereof) is used. We note that an analogue of this idea takes place in $\mathbb{F}_p$ using the point-line incidence bound of Stevens-de Zeeuw [20] in place of the Szemerédi-Trotter theorem, which naturally produces a bound on the fourth moment energy. For a convex function f, this trick changes as follows: we can obtain bounds on $\mathsf{E}_3^+(f(A),B)$ if we have *additive* structure on A, say $r_{Q-A}(a) \geqslant T$ for all $a \in A$.

To benefit from the 'enhanced energy trick' described above, we need the appropriate data on Q, R and T. A generic technique for this, first described in [12] and refined in [18], yields a subset $C \subseteq A$ with suitable parameters: that is, if $\mathsf{E}_3^+(A) \sim |D_t|t^3$ for some $D_t \subseteq A - A$, then $r_{D_t - A}(c) \geqslant |D_t|t|A|^{-1}$, and $|C| \geqslant |D_t|t|A|^{-1}$. A recent expository lemma of Xue [21] enhances the strength of this result, to enable one to take $|C| \gtrsim |A|$ - we use an adaptation of this regularisation result.

We conclude this section by considering where improvements to these techniques may be found. Certainly for the real numbers, there is hope that one could find a more optimised subset of A, with the data on Q, R and T optimised for the specific applications within our paper. Indeed, such a 'better subset' is present in the current bounds for the sum-product problem [13]). In [13], an elementary, somewhat geometric, argument justifies the existence of the subset used in the context of the sum-product problem.

The third item of our list might also be improved as follows: we bound the number of solutions to $a - b = (a + c) - (b + c)$ in terms of the third moment energy. During this argument, we use Cauchy-Schwarz to bound a factor of $\mathsf{E}_{3/2}^+(A, \cdot)$ which appears as a by-product of Hölder's inequality. However, it may be possible to directly bound $\mathsf{E}_{3/2}^+(A, \cdot)$ using other methods. For example, if A is a convex set, then Solymosi and Ruzsa [14] show that $\mathsf{E}_{3/2}^+(A,B) \ll |A + B|^{3/2}$ for any set B.

In the proof of Theorem 11, we (implicitly) turn to the recent technique of studying the *line energy* (see e.g. [7, 9]). We would not be surprised if future developments of this concept provide further tools relevant to the results in this paper.

1 Preliminaries

We use the notation $r_{Q-R}(a)$ to denote the number of representations of the element a as a difference from $Q - R$, that is, $r_{Q-R}(a) = |\{(q, r) \in Q \times r : q - r = a\}|$, and similarly for $r_{QR}(a)$ etc. The kth moment additive energy between sets A and B is defined to be

$$\mathsf{E}_k^+(A,B) := \sum_{x\in A-B} r_{A-B}^k(x)$$

for $k \geqslant 1$. If $A = B$ we simply write $\mathsf{E}_k^+(A)$. Similarly, we define the multiplicative energy $\mathsf{E}_k^\times(A,B) := \sum_x r_{A/B}^k(x)$, where we assume that $0 \notin B$.

1.1 Energy Bounds via Szemerédi - Trotter

Before beginning the proofs, we require some technical lemmas. The first gives a bound for the additive energy of two sets A and B, subject to multiplicative information on the set A, and can be found in [13]. We give the proof for completeness, noting that the proof for Lemma 13 follows from a similar argument.

Lemma 12. *Let $A, B, C, Q, R \subset \mathbb{R}$ be finite sets with the property that $r_{QR}(a) \geqslant T$ for all $a \in A$ and some $T \geqslant 1$. Then if $|R||C| \ll (|Q||B|)^2$,*

$$|\{(a,b,c) \in A \times B \times C : c = a - b\}| \ll \frac{(|Q||R||B||C|)^{2/3}}{T}. \tag{1}$$

Furthermore, if $|R||A| \leqslant |Q|^2|B|$,

$$\mathsf{E}_3^+(A,B) \ll \frac{|Q|^2|R|^2|B|^2}{T^3}\log|A|. \tag{2}$$

The next lemma bounds the additive energy of two sets $f(A)$ and B, where f is a convex function, subject to additive information on the set A.

Lemma 13. *Let $A \subset \mathbb{R}$ be finite, and let f be a convex (or concave) function. Suppose that there exist finite sets $Q, R \subseteq \mathbb{R}$ with $|Q| \geqslant |R|$ and a number $T \geqslant 1$ so that $r_{Q-R}(a) \geqslant T$ for all $a \in A$. Then for any set B satisfying $|R||A| \ll |Q|^2|B|$, we have*

$$\mathsf{E}_3^+(f(A),B) \ll \frac{|Q|^2|R|^2|B|^2}{T^3}\log|A|.$$

We remark that we have stated Lemmas 12 and 13 as a *third* energy bound. The same technique with an additional interpolation argument gives us kth moment energy bounds, see e.g. [13] for details.

Proof of Lemma 12. To prove the first bound, we note that by utilising the information on the sets Q and R, we have

$$|\{(a,b,c) \in A \times B \times C : c = a - b\}| \leqslant \frac{1}{T}|\{(q,r,b,c) \in Q \times R \times B \times C : c = qr - b\}|,$$

which can be viewed as incidences between the set of lines L given by $y = qx - c$ for $(q,c) \in Q \times C$, and the point set $P = R \times B$. Applying the Szemerédi - Trotter theorem, we have

$$|\{(q,r,b,c) \in Q \times R \times B \times C : c = qr - b\}| = I(P,L) \ll (|Q||R||B||C|)^{2/3} + |Q||B|.$$

Because of the constraint present in the statement of the lemma, the leading term dominates. We therefore have

$$|\{(a,b,c) \in A \times B \times C : c = a - b\}| \ll \frac{(|Q||R||B||C|)^{2/3}}{T}$$

as needed.

For the second part of the lemma, we decompose the support of $\mathsf{E}_3^+(A,B)$ into dyadic ranges: for $i = 0, \dots \lfloor \log |A| \rfloor$, let $D_i := \{d \in A - B : r_{A-B}(d) \in [2^i, 2^i)\} \subseteq A - B$. Then

$$\mathsf{E}_3^+(A,B) = \sum_{i=0}^{\lfloor |A| \rfloor} \sum_{d \in D_i} r_{A-B}^3(d) < \sum_i |D_i| 2^{3i+3} \ll \log |A| \max_i |D_i| 2^{3i} .$$

With D_i playing the role of C in (1), we have

$$2^i |D_i| \leqslant |\{(a,b,d) \in A \times B \times D_i : d = a - b\}| \ll \frac{(|Q||R||B||D_i|)^{2/3}}{T} .$$

The result then follows, and all that is left to do is to verify the condition required, for $C = D_i$, i.e. that $|Q||D_i| \ll (|R||B|)^2$. Note that since $D_i \subseteq A - B$, this is certainly true if we have

$$|Q||A||B| \ll (|R||B|)^2 \iff |Q||A| \ll |R|^2 |B|$$

which is the stated condition. □

1.2 Regularisation Results

In this section we give some regularisation results required for the proof. The first is a lemma present in [13]. This lemma will be used to give a certain subset of A on which much of the energy is supported, and with certain popularity properties.

Lemma 14. *Let $\mathcal{R}_\epsilon$ be a map with parameter $\epsilon \in (0,1)$ that, to every sufficiently large finite additive set X, associates a subset $\mathcal{R}_\epsilon(X) \subseteq X$ of cardinality $|\mathcal{R}_\epsilon(X)| \geqslant (1-\epsilon)|X|$.*

For any such map $\mathcal{R}_\epsilon$, any $m > 1$ and a sufficiently large finite set A, set $\epsilon = c_1 \log^{-1}(|A|)$ for some $c_1 \in (0,1)$. Then there exists a set $B \subseteq A$ (depending on $\mathcal{R}_\epsilon$, m), with $|B| \geqslant (1-c_1)|A|$ such that

$$\mathsf{E}_m^+(\mathcal{R}_\epsilon(B)) \geqslant c_2\, \mathsf{E}_m^+(B) ,$$

for some constant $c_2 = c_2(m, c_1)$ in $(0,1]$.

We also require the following proposition. It is very similar to an expository lemma of Xue [21, Lemma 5.1], but has been amended to admit an asymmetric form. We present the rather technical proof of this proposition in the appendix, where we make the dependence on $\log(|A|)$ and k hidden in the notation explicit.

Proposition 15. *Let A, V be finite subsets of $\mathbb{R}$, let $k > 1$ be a real number and fix $c_1 \in (0, 1)$.*

Then there are sets B, C with $C \subseteq B \subseteq A$ and $|C| \gtrsim_{k,c_1} |B| \geqslant (1 - c_1)|A|$ such that the following property holds: there is a number $1 \leqslant t \leqslant |B|$ and a set $D_t = \{x \in B - V : t \leqslant r_{B-V}(x) < 2t\}$ such that

$$\mathsf{E}_k^+(B, V) \sim_k |D_t|t^k$$

and

$$r_{D_t+V}(c) \sim_k \frac{|D_t|t}{|B|}$$

for any $c \in C$.

On a high level, the proofs of Lemma 14 and Proposition 15 follow the same scheme: given a set A, we define a map which extracts a positive proportion subset $A' \subseteq A$ with desirable properties. In Lemma 14, this map is abstract, whereas in Proposition 15 it is explicit. We then iterate this procedure until some stopping condition is satisfied. In Lemma 14, this stopping condition is relative to the mth energy; in Proposition 15, the stopping condition is defined with respect to the *support* of the kth energy. These two regularisation results differ primarily because of this subtlety. Finally, we argue that this procedure must terminate in an acceptable number of steps, thus eventually outputting a positive proportion subset $B \subseteq A$.

Proposition 15 admits the following corollary, which is similar to a result of Shakan [16, Theorem 1.10].

Corollary 16. *Let $A, V \subseteq \mathbb{R}$ be finite, and f be a convex (or concave) function. Then there are sets B, C with $C \subseteq B \subseteq A$ and $|C| \gtrsim |B| \gg |A|$ such that*

$$\mathsf{E}_3^+(B, V)\mathsf{E}_3^+(f(C), U) \lesssim |U|^2|V|^2|A|^3$$

for any set U with $|U||V| \gg |A|$.

Proof. We apply Proposition 15 with $k = 3$ to obtain the sets B and C, so that $\mathsf{E}_3^+(B, V) \sim |D_t|t^3$ where $r_{B-V}(d) \in [t, 2t)$ for all $d \in D_t$ and $r_{D_t+V}(c) \gg |D_t|t|B|^{-1}$ for all $c \in C$.

We are able to obtain a bound on $\mathsf{E}_3^+(f(C), U)$ using Lemma 13:

$$\mathsf{E}_3^+(f(C), U) \lesssim \frac{|D_t|^2|V|^2|U|^2}{|D_t|^3t^3|B|^{-3}} \sim \frac{|V|^2|U|^2|A|^3}{\mathsf{E}_3^+(B, V)}.$$

We remark that since $|U||V| \gtrsim |A|$, it follows that $\min(|D_t|, |V|)|C| \lesssim \max(|D_t|, |V|)^2|U|$ and so we may indeed apply Lemma 13. $\square$

2 Auxiliary energy bounds

A unifying idea behind the proofs in this paper is the following proposition:

Proposition 17. *Let $A, C \subseteq \mathbb{R}$ be finite, and $k \geqslant 1$. Suppose that $\mathsf{E}_k^+(A) \sim |D|\Delta^k$ for some $D \subseteq A - A$ and $\Delta \geqslant 1$, where $r_{A-A}(d) \in [\Delta, 2\Delta)$. Then we have*

$$|D|^9\Delta^{12} \lesssim \frac{|A+C|^6\mathsf{E}_3^+(A)^4\mathsf{E}_3^+(C)^2\mathsf{E}_3^+(A,D)\mathsf{E}_3^+(C,A+C)^2}{|C|^{18}|A|^3}. \tag{3}$$

The stated form of Proposition 17 gives us a great deal of flexibility. For example, if we had multiplicative information on the set A in the guise of Lemma 13 – that is, if $r_{QR}(a) \geqslant T$ for all $a \in A$ – then we obtain an energy estimate in terms of this data. Proposition 17 also admits a multiplicative form, in which $\mathsf{E}_k^\times(A) \sim |D|\Delta^k$. Then all instances of E_3 in (3) should be replaced by $\mathsf{E}_3^\times$, and $A+C$ by AC.

Proof. We begin by defining the popular set

$$P(A,C) := \left\{x \in A+C : r_{A+C}(x) \geqslant \frac{|A||C|}{\log|A||A+C|}\right\}.$$

We also define the set

$$A' := \left\{a \in A : |\{c \in C : a+c \in P(A,C)\}| \geqslant \frac{|C|}{2}\right\}.$$

We perform a refinement step at the beginning of the proof, making use of Lemma 14. We claim that Lemma 14 can be applied with the map $\mathcal{R}_\epsilon$ giving the subset $A' \subseteq A$ defined above. Firstly we prove that $|A'|$ is large with respect to $|A|$. We have

$$\begin{aligned}\sum_{a\in A'} |\{c \in C : a+c \in P(A,C)\}| + \sum_{a \in A\setminus A'} &|\{c \in C : a+c \in P(A,C)\}| \\ &= |\{(a,c) \in A \times C : a+c \in P(A,C)\}| \\ &\geqslant \left(1 - \frac{1}{\log|A|}\right)|A||C|.\end{aligned}$$

By setting $|A \setminus A'| = c|A|$ and using the bounds

$$\sum_{a\in A'} |\{c \in C : a+c \in P(A,C)\}| \leqslant (1-c)|A||C|$$

$$\sum_{a\in A\setminus A'} |\{c \in C : a+c \in P(A,C)\}| \leqslant \frac{c}{2}|A||C|$$

we conclude that $|A'| \geqslant \left(1 - \frac{2}{\log|A|}\right)|C|$. We can therefore apply Lemma 14 at the outset of the proof, obtaining a set A' as above with the property that $|A'| \gtrsim |A|$, and $\mathsf{E}_k^+(A') \sim \mathsf{E}_k^+(A)$.

We now consider the number of solutions $(a,b,c) \in A^2 \times C$ to the trivial equation

$$a - b = (a+c) - (b+c) \tag{4}$$

where the difference $a-b$ comes from the set $D \subseteq A'-A'$ such that $|D|\Delta^k \sim \mathsf{E}_k^+(A') \sim \mathsf{E}_k^+(A)$, and such that the sum $a+c$ is popular, that is, $a+c \in P(A,C)$.

There are at least $\Omega(|C||D|\Delta)$ solutions to equation (4). We partition solutions to (4) with the relevant conditions, via the following:

$$(a,b,c) \sim (a+t, b+t, c-t), \quad t \in \mathbb{R}\,,$$

and let $[a,b,c]$ represent this equivalence class. Since t cancels out in equation (4), these classes are non-trivial.

Let N denote the number of solutions to equation (4). We have

$$|C||D|\Delta \ll N = \sum_{[a,b,c]} |[a,b,c]|$$

and so, after an application of the Cauchy-Schwarz inequality, we obtain

$$(|C||D|\Delta)^2 \leqslant |\{\text{equivalence classes}\}| \cdot \sum_{[a,b,c]} |[a,b,c]|^2. \tag{5}$$

We now aim to bound the two factors in equation (5).

To bound the number of equivalence classes, note that each equivalence class gives a solution to the equation

$$d = s_1 - s_2, \quad d \in D, s_1 \in P(A,C), s_2 \in A+B.$$

Therefore we have

$$|\{\text{equivalence classes}\}| \leqslant |\{(d,s_1,s_2) \in D \times P(A,C) \times A+C : d = s_1 - s_2\}|.$$

By the popularity of s_1, we have

$$\begin{aligned} |\{\text{equivalence classes}\}| &\lesssim \frac{|A+C|}{|A||C|} |\{(d,a,c,s) \in D \times A \times C \times A+C : d-a = c-s\}| \\ &= \frac{|A+C|}{|A||C|} \sum_x r_{D-A}(x) r_{C-(A+C)}(x) \\ &\leqslant \frac{|A+C|}{|A||C|} \mathsf{E}_3^+(A,D)^{\frac{1}{6}} (|A||D|)^{\frac{1}{2}} \mathsf{E}_3^+(C,A+C)^{\frac{1}{3}}\,, \end{aligned}$$

where the final bound is an application of Hölder's inequality, followed by Cauchy-Schwarz. We now aim to bound the sum

$$\sum_{[a,b,c]} |[a,b,c]|^2$$

where it is understood that the sum is taken over equivalence classes satisfying the relevant conditions. Note that this sum counts pairs of triples from the same equivalence class, and for each pair we have

$$(a,b,c) \sim (a',b',c') \implies \exists\, t \text{ with } a-a' = b-b' = c'-c = t.$$

We therefore have

$$\sum_{[a,b,c]} |[a,b,c]|^2 \leqslant \sum_t r_{A-A}(t)^2 r_{C-C}(t) \leqslant \mathsf{E}_3^+(A)^{\frac{2}{3}} \mathsf{E}_3^+(C)^{\frac{1}{3}}$$

where again, the final inequality is a result of Hölder's estimate. Finally, from (5) we have

$$(|C||D|\Delta)^2 \lesssim \frac{|A+C|}{|A||C|} \mathsf{E}_3^+(A,D)^{\frac{1}{6}} (|A||D|)^{\frac{1}{2}} \mathsf{E}_3^+(C, A+C)^{\frac{1}{3}} \mathsf{E}_3^+(A)^{\frac{2}{3}} \mathsf{E}_3^+(C)^{\frac{1}{3}} .$$

Rearranging and raising both sides to the sixth power concludes the proof. □

3 Proof of Theorem 6

We actually prove the following, slightly more general theorem.

Theorem 18. *Let f and g be convex or concave functions. Let $A, B \subseteq \mathbb{R}$ be finite sets. Then we have*

$$|A|^{49}|B|^{49} \lesssim |A+B|^{38}|f(A)+g(B)|^{38} \tag{6}$$

and

$$|A|^{39}|B|^{39} \lesssim |A \pm B|^{20}|f(A) \pm g(B)|^{20}|A-A|^5||B-B|^5|f(A)-f(A)|^5|g(B)-g(B)|^5 . \tag{7}$$

We clarify that in this theorem, one may take f to be convex, and g to be concave.

On a high level, the proof proceeds by applying two iterations of Corollary 16 to A and B with judicious choices of V in each case. Then we apply Proposition 17 to the ensuing subsets and their convex (resp. concave) counterparts. This gives an additive energy relation. We obtain the statements of Theorem 18 using Cauchy-Schwarz and Hölder inequalities.

Let us make two simple observations regarding the third moment energy of a set X that we use in the subsequent argument. Firstly, note that $\mathsf{E}_3^+(-X, X-X) = \mathsf{E}_3^+(X, X-X)$ due to the symmetry of the difference set. Secondly, for any set $Y \subseteq X$ and any set Z, we have $\mathsf{E}_3^+(Y,Z) \leqslant \mathsf{E}_3^+(X,Z)$.

Proof. Here we prove the slightly more technical statement (6), and indicate the changes necessary to prove (7). We begin by applying Corollary 16 to the set A with $V = A$ to obtain sets $A_2 \subseteq A_1 \subseteq A$ with $|A_2| \gtrsim |A_1| \gg |A|$ and

$$\mathsf{E}_3^+(A_1, A)\mathsf{E}_3^+(f(A_2), U) \lesssim |A|^5|U|^2 \text{ for any } U .$$

Note that if $|U| \gg 1$, then this follows from Corollary 16; if $|U| \ll 1$, then it follows trivially.

We now apply the concave analogue of Corollary 16, this time to the set $f(A_2)$ with $V = f(A)$ and the function f^{-1}. We obtain [3] the sets $A_4 \subseteq A_3 \subseteq A_2$ with $|A_4| \gtrsim |A_3| \gg |A_2| \gtrsim |A|$ so that

$$\mathsf{E}_3^+(f(A_3), f(A))\mathsf{E}_3^+(A_4, U) \lesssim |A|^5|U|^2 \text{ for any } U .$$

[3]Strictly speaking, we obtain sets $f(A_4) \subseteq f(A_3) \subseteq f(A_2)$.

We repeat this argument for the set B taking $V = B$ to obtain $B_2 \subseteq B_1 \subseteq B$ so that

$$\mathsf{E}_3^+(B_1, B)\mathsf{E}_3^+(g(B_2), U) \lesssim |B|^5|U|^2 \text{ for any } U\,,$$

and then once more to $g(B_2)$ with $V = g(B)$ and function g^{-1} to obtain $B_4 \subseteq B_3 \subseteq B_2$ with $|B_4| \gtrsim |B|$ and

$$\mathsf{E}_3^+(g(B_3), g(B))\mathsf{E}_3^+(B_4, U) \lesssim |B|^5|U|^2 \text{ for any } U\,.$$

To prove (6), we dyadically decompose with relation to the sets $A_4, B_4, f(A_4), g(B_4)$, according to the second moment energy to obtain sets D_i and numbers $t_i \geqslant 1$ so that

$$\mathsf{E}_2^+(A_4) \sim |D_1|t_1^2, \quad \mathsf{E}_2^+(B_4) \sim |D_2|t_2^2$$
$$\mathsf{E}_2^+(f(A_4)) \sim |D_3|t_3^2, \quad \mathsf{E}_2^+(g(B_4)) \sim |D_4|t_4^2\,.$$

To prove (7), we would instead dyadically decompose according to the 12/7th moment energy, so that e.g. $\mathsf{E}_{12/7}^+(A_4) \sim |D_1|t_1^{12/7}$. Note that e.g. $D_1 \subseteq A_4 - A_4$.

We now apply Proposition 17 to each of the sets $A_4, B_4, f(A_4), g(B_4)$, choosing C in (3) to be $B_4, A_4, g(B_4), f(A_4)$ respectively.

We then multiply together the four instances of (3) obtained from these applications, and make liberal use of the simple observations noted at the beginning of this section together with the consequences of Corollary 16, which allows us to match up energies on the right hand side and bound them to get an equation with no energies present. After a lengthy calculation, we obtain the following.

$$\prod_{1\leqslant i\leqslant 4} |D_i|^7 t_i^{12} \lesssim |A+B|^{20}|f(A)+g(B)|^{20}|A|^9|B|^9\,. \tag{8}$$

To prove statement (7), we recall that we had initially dyadically decomposed according to the 12/7th energy and so, after an application of Hölder's inequality for $\mathsf{E}_{12/7}^+(A_4)$ etc., we are done.

To prove statement (6), let us multiply (8) on both sides by $(t_1t_2t_3t_4)^2$. Note that

$$|D_1|t_1^3|D_3|t_3^3 \leqslant \mathsf{E}_3^+(A_4, A)\mathsf{E}_3^+(f(A_3), f(A)) \lesssim |A|^7 \implies t_1t_2 \lesssim \frac{|A|^7}{\mathsf{E}_2^+(A)\mathsf{E}_2^+(f(A))}$$

and similarly

$$(t_2t_4) \lesssim \frac{|B|^7}{\mathsf{E}_2^+(B)\mathsf{E}_2^+(g(B))}.$$

Hence we obtain

$$\left(\mathsf{E}_2^+(B)\mathsf{E}_2^+(g(B))\mathsf{E}_2^+(A)\mathsf{E}_2^+(f(A))\right)^9 \lesssim |A+B|^{20}|f(A)+g(B)|^{20}|A|^{23}|B|^{23}\,.$$

Finally, we use the Cauchy-Schwarz relation

$$\frac{|X|^2|Y|^2}{|X+Y|} \leqslant \mathsf{E}_2^+(X,Y) \leqslant \mathsf{E}_2^+(X)^{1/2}\mathsf{E}_2^+(Y)^{1/2}$$

to complete the proof. □

4 Proof of Theorem 11

In this section we prove Theorem 11 proving two complementary bounds, using a combination of the methods found in [10], [13], and [9].

4.1 Proof of Theorem 11 - Bound 1

The method of Roche-Newton and Warren [9] involved studying the *line energy* of lines of a particular structure - this notion was first developed by Elekes, see for instance [1]. Their results, combined with an incidence theorem of Rudnev and Shkredov [11] and an additive combinatorial result of Roche-Newton and Rudnev[4] [8] imply the following incidence bound. See also [7] for more information on line energy and its applications.

Theorem 19. *Let L be a set of lines of the form $y = ax + a'$ for $a, a' \in A \subseteq \mathbb{R} \setminus \{0\}$ a finite set. Let $B, C \subseteq \mathbb{R}$ be two finite sets. Then we have*

$$\mathcal{I}(B \times C, L) \lesssim \mathsf{E}_4^{\times}(A)^{\frac{1}{12}}|A|^{\frac{7}{6}}|B|^{\frac{2}{3}}|C|^{\frac{1}{2}} + |A|^2|C|^{\frac{1}{2}}.$$

We shall apply Theorem 19 to the point set $B \times (AB + A)$ and to the set of lines L of the form $y = ax + a'$ with $a, a' \in A$. Note that without loss of generality we may remove 0 from A if it is present. For each line $y = ax + a'$, for each $b \in B$ the point $(b, ab + a')$ lies on this line, and so we have at least $|A|^2|B| \sim |A|^3$ incidences. Using Theorem 19 we obtain

$$|A|^3 \lesssim \mathcal{I}(B \times (AB + A), L) \lesssim \mathsf{E}_4^{\times}(A)^{\frac{1}{12}}|A|^{\frac{7}{6}}|B|^{\frac{2}{3}}|AB + A|^{\frac{1}{2}} + |A|^2|AB + A|^{\frac{1}{2}}. \quad (9)$$

Note that if the second term dominates we have a much stronger result than claimed in the statement in Theorem 11. Let us therefore assume the first term dominates. Hence we have the first of our two bounds:

$$|A|^{7/3} \lesssim |AB + A|\mathsf{E}_4^{\times}(A)^{1/6} \leqslant |AB + A||A|^{\frac{1}{6}}\mathsf{E}_3^{\times}(A)^{1/6}. \quad (10)$$

4.2 Proof of Theorem 11 - Bound 2

To find the second bound, let us apply the multiplicative version of Proposition 15 to the set A with $V = A$ to obtain sets $A_2 \subseteq A_1 \subseteq A$ with $|A_2| \gtrsim |A_1| \gg |A|$ so that

$$\mathsf{E}_3^{\times}(A_1, A)\mathsf{E}_3^{+}(A_2, U) \lesssim |A|^5|U|^2\,. \quad (11)$$

Equation (11) is a consequence of using Lemma 12 in place of Lemma 13 in the proof of Corollary 16.

[4] The result of Roche-Newton and Rudnev is that the number of solutions to the equation

$$\frac{a_1 - a_2}{a_3 - a_4} = \frac{a_5 - a_6}{a_7 - a_8}$$

with each $a_i \in A$ is at most $O(|A|^6 \log |A|)$.

We now apply Proposition 17 to the set A_2, writing $\mathsf{E}_2^+(A_2) \sim |D|t^2$ and taking $C = \lambda A_2$ for $\lambda \neq 0$. Note that $\mathsf{E}_k^+(A_2, X) = \mathsf{E}_k^+(\lambda A_2, \lambda^{-1}X)$ for any set X and any $k \geqslant 1$.

From Proposition 17, (11), and the inclusions $A_2 \subseteq A_1 \subseteq A$ we obtain

$$\begin{aligned} |D|^7 t^{12} &\lesssim \frac{|A+\lambda A|^{10}}{|A|^9} \left(\frac{\mathsf{E}_3^+(A_2)}{|A|^2}\right)^{12} \frac{\mathsf{E}_3^+(A_2, D)}{|D|^2} \left(\frac{\mathsf{E}_3^+(A_2, \lambda^{-1}A + A}{|A+\lambda A|^2}\right)^2 \\ &\lesssim \frac{|A+\lambda A|^{10}}{|A|^9} \frac{|A|^{45}}{\mathsf{E}_3^\times(A_1, A)^9} . \end{aligned} \tag{12}$$

We have

$$|D|t^3 \leqslant \mathsf{E}_3^+(A_2) \lesssim \frac{|A|^7}{\mathsf{E}_3^\times(A_1, A)} \implies t \lesssim \frac{|A|^7}{\mathsf{E}_3^\times(A_1, A)\mathsf{E}_2^+(A_2)},$$

and so multiplying (12) by t^2 and applying the Cauchy-Schwarz energy bound

$$\frac{|A_2|^4}{|A_2 + \lambda A_2|} \leqslant \mathsf{E}(A_2, \lambda A_2) \leqslant \mathsf{E}(A_2)$$

we conclude that

$$|A + \lambda A|^{19} \gtrsim \frac{\mathsf{E}_3^\times(A_1, A)^{11}}{|A|^{14}} . \tag{13}$$

4.3 Proof of Theorem 11 - Conclusion

Combining the bounds of the previous section we obtain

$$|A + BA| \gtrsim \max\left(\frac{\mathsf{E}_3^\times(A, A_1)^{\frac{11}{19}}}{|A|^{\frac{14}{19}}}, \frac{|A|^{\frac{13}{6}}}{\mathsf{E}_3^\times(A, A_1)^{\frac{1}{6}}}\right)$$

where the first bound has instead been applied to the set A_1 given above, making use of the inequalities $|A| \ll |A_1| \ll |A|$ and $\mathsf{E}_3^+(A_1) \leqslant \mathsf{E}_3^+(A, A_1)$. In the worst possible case, both maximands are equal. This happens if

$$\mathsf{E}_3^+(A_1, A) = |A|^{\frac{331}{85}}$$

and so we shall assume that this is indeed the case. We then obtain

$$|A + BA| \gtrsim |A|^{\frac{129}{85}} = |A|^{\frac{3}{2} + \frac{3}{170}}$$

as required.

Acknowledgements

The authors were supported by Austrian Science Fund FWF Project P 30405-N32. We are especially grateful to Oliver Roche-Newton who pushed us to improve our results. We also thank Misha Rudnev for helpful suggestions. We are very grateful to the anonymous referees for useful comments and suggestions.

References

[1] G. Elekes, *On linear combinatorics I. Concurrency An algebraic approach*, Combinatorica, 17, 447-458 (1997).

[2] G. Elekes, M. Nathanson, and I. Ruzsa, *Convexity and sumsets*, J. Number Theory, 83, 194–201 (1999).

[3] B. Hanson, O. Roche-Newton, and M. Rudnev, *Higher convexity and iterated sum sets*, Combinatorica (2021).

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

[5] L. Li and O. Roche-Newton, *Convexity and a sum-product type estimate*, Acta Arith. 156(3), 247–255 (2012).

[6] B. Murphy, *Upper and lower bounds for rich lines in grids*, Amer. J. Math. 143, 2, 577-611 (2021).

[7] G. Petridis, O. Roche-Newton, M. Rudnev, and A. Warren, *An energy bound in the affine group*, Int. Math. Res. Not. (2020).

[8] O. Roche-Newton and M. Rudnev, *On the Minkowski distances and products of sum sets*, Israel J. Math, 209, no. 2, 507-526 (2015).

[9] O. Roche-Newton and A. Warren, *New expander bounds from affine group energy*, Discrete & Comput. Geom. (2020).

[10] M. Rudnev, G. Shakan, and I. D. Shkredov, *Stronger sum-product inequalities for small sets*, Proc. Amer. Math. Soc. 148, 1467-1479 (2020).

[11] M. Rudnev and I. D. Shkredov, *On growth rate in $SL_2(\mathbb{F}_p)$, the affine group and sum-product type applications*, arXiv:1812.01671 (2018).

[12] M. Rudnev, I. D. Shkredov and S. Stevens, *On the energy variant of the sum-product conjecture,* Rev. Mat. Iberoam. **36**:1, 207–232 (2020).

[13] M. Rudnev and S. Stevens, *An update on the sum-product problem*, Math. Proc. Cambridge Philos. Soc. 1-20 (2021).

[14] I. Ruzsa and J. Solymosi, *Sumsets of semiconvex sets*, Canad. Math. Bull. 1-11 (2021).

[15] T. Schoen and I. D. Shkredov, *On sumsets of convex sets*, Combin. Probab. Comput. 20 (5), 793-798 (2011).

[16] G. Shakan, *O*n higher energy decompositions and the sum-product phenomenon, Math. Proc. Cambridge Phil. Soc. **167**:3, 599–617 (2019).

[17] I. D. Shkredov, *On sums of Szemerédi-Trotter sets*, Proc. Steklov Inst. Math. 289, 300309 (2015).

[18] I. D. Shkredov, *Some remarks on the Balog-Wooley decomposition theorem and quantities D^+, $D^\times$,* Proc. Steklov Inst. Math. 298, 74-90 (2017).

[19] J. Solymosi, *Bounding multiplicative energy by the sumset*. Adv. Math. **222** no. 2, 402-408 (2009).

[20] S. Stevens and F. de Zeeuw, *An improved pointline incidence bound over arbitrary fields*, Bull. Lond. Math. Soc. 49: 842-858 (2017).

[21] B. Xue, *Asymmetric estimates and the sum-product problems*, arXiv:2005.09893 (2020).

Appendix - Proof of Proposition 15

We present the proof of Proposition 15 in this section.

Proposition 20. *Let $k > 1$ be a given real number. Fix $c_1 \in (0,1)$, and let A, V be finite subsets of $\mathbb{R}$. Then there are sets B, C with $C \subseteq B \subseteq A$ and $|C| \gtrsim_{k,c_1} |B| \geqslant (1-c_1)|A|$, such that the following property holds: there is a number $1 \leqslant t \leqslant |B|$ and a set $D_t = \{x \in B - V : t \leqslant r_{B-V}(x) < 2t\}$ such that*

$$|D_t|t^k \leqslant \mathsf{E}_k^+(B,V) \leqslant 2^k |D_t| t^k \log(|B|)$$

and

$$r_{D_t+V}(c) \in \left[\frac{|D_t|t}{2^{k+1}|B|}, \frac{2|D_t|t}{|B|}\frac{k2^k \log^2|A|}{c_1}\right]$$

for any $c \in C$.

Here, the subscripts in $\gtrsim_k$, $\gg_k$ or $\approx_k$ means that the implied constant may depend on k.

Proof. The proof of this lemma is two-fold: first we will refine the set A iteratively according to a map $\mathcal{R}_\varepsilon$ for a fixed $\varepsilon > 0$. This yields a set $B \subseteq A$ so that $|B| \geqslant (1-\varepsilon)|A|$. We then choose $C \subseteq \mathcal{R}_\varepsilon(B)$ and argue that the iteration process guarantees that C has the desired properties.

Let us first describe the map applied to a dummy set $\tilde{A}$. We begin by dyadically decomposing $\tilde{A} - V$ to obtain $D_t \subseteq \tilde{A} - V$ and a number $1 \leqslant t \leqslant \min(|\tilde{A}|, |V|)$ so that $|D_t|t^k \leqslant \mathsf{E}_k^+(\tilde{A}, V) \leqslant \log(\min(|\tilde{A}|, |V|))|D_t|t^k$ and $r_{\tilde{A}-V}(d) \in [t, 2t)$ for any $d \in D_t$. That is, we perform a dyadic decomposition argument according to the kth energy. We also define the set

$$\mathcal{P}_{\tilde{A}} := \left\{(a,v) \in \tilde{A} \times V : a - v \in D_t\right\},$$

which is the set of points of $\tilde{A} \times V$ supported on lines with slope in D_t. By construction, we have that $|\mathcal{P}_{\tilde{A}}| \in [|D_t|t, 2|D_t|t)$. Now, with $\varepsilon > 0$ a parameter, define a subset

$$\mathcal{R}_\varepsilon(\tilde{A}) := \left\{a \in \tilde{A} : r_{D_t+V}(a) \leqslant \frac{|\mathcal{P}_{\tilde{A}}|}{\varepsilon|\tilde{A}|}\right\}.$$

We claim that $|\mathcal{R}_\varepsilon(\tilde{A})| \geqslant (1-\varepsilon)|\tilde{A}|$. Indeed, writing $\tilde{A}' = \mathcal{R}_\varepsilon(\tilde{A})$, we have

$$|\tilde{A} \setminus \tilde{A}'|\frac{|\mathcal{P}_{\tilde{A}}|}{\varepsilon|\tilde{A}|} \leqslant |\{(a,v) \in \mathcal{P}_{\tilde{A}} : a \notin \tilde{A}'\}| \leqslant |\mathcal{P}_{\tilde{A}}|$$

and it follows that $|\tilde{A}'| > (1-\varepsilon)|\tilde{A}|$.

We now describe the iteration scheme in the proof using the notation introduced above: let $A_0 = A$ and for $i \geqslant 0$ define

$$G_i := \mathcal{P}_{A_i} \cap (\mathcal{R}_\varepsilon(A_i) \times V) = \{(a,v) \in \mathcal{R}_\varepsilon(A_i) \times V : a - v \in D_t(A_i)\}$$

where $D_t(A_i) \subseteq A_i - V$ is the set supporting the kth energy $\mathsf{E}_k^+(A_i, V)$. If $|G_i| < 2^{-k}|\mathcal{P}_{A_i}|$ then set $A_{i+1} = \mathcal{R}_\varepsilon(A_i)$. Otherwise we terminate the process and set $B = A_i$ and $C' = \mathcal{R}_\varepsilon(A_i)$. Note that $|A_i| \geqslant (1-\varepsilon)^i|A| \geqslant (1-i\varepsilon)|A|$. We remark that the stopping condition of this algorithmic procedure differs from the stopping condition in Proposition 17. We claim that this process must terminate in fewer than $I = c_1\varepsilon^{-1}$ steps. For ease of notation, let us suppose that $c_1\varepsilon^{-1} \in \mathbb{N}$. Indeed, suppose for contradiction that we are in the Ith step of the process. Then we have a set $A_I \subseteq A$ so that $|A_I| \geqslant (1-c_1)|A|$ and for each $0 \leqslant i \leqslant I$ we have $|G_i| < 2^{-k}|\mathcal{P}_{A_i}|$.

Let us write D_i to mean $D_t(A_i)$ - that is $\mathcal{P}_{A_i} = \{(a, v) \in A_i \times V : a - v \in D_i\}$. Similarly, let us write the t corresponding to D_i as t_i so that $\mathsf{E}_k^+(A_i, V) \in [|D_i|t_i^k, 2^k|D_i|t_i^k \log(|A_i|))$.

Since we have not terminated the iteration procedure, we obtain for each $0 \leqslant i \leqslant I-1$ that

$$\begin{aligned}\sum_{x \in D_i} r^k_{\mathcal{R}_\varepsilon(A_i)-V}(x) &\leqslant (2t_i)^{k-1}\,|\mathcal{P}_{A_i} \ \cap\ (\mathcal{R}_\varepsilon(A_i) \times V)| = (2t_i)^{k-1}|G_i| \\ &< 2^{-k}(2t_i)^{k-1}|\mathcal{P}_{A_i}| = t_i^{k-1}|\mathcal{P}_{A_i}|/2\end{aligned}$$

Let us now consider the number of terms in the support of the energy that we discard during the iteration process:

$$\begin{aligned}|\{((a_1, v_1), \ldots, (a_k, v_k)) \in (\mathcal{P}_{A_i} \setminus G_i)^k \colon a_1 - v_1 = \cdots = a_k - v_k\}| \\ = \sum_{x \in D_i} r^k_{A_i - V}(x) - \sum_{x \in D_i} r^k_{\mathcal{R}_\varepsilon(A_i)-V}(x) \\ \geqslant t_i^{k-1}|\mathcal{P}_{A_i}|/2 \\ \geqslant |D_i|t_i^k \\ \geqslant 2^{-k}\mathsf{E}_k^+(A_i, V)\log(|A_i|)^{-1}\end{aligned}$$

We emphasise that any discarded energy-term $((a_1, v_1), \ldots, (a_k, v_k))$ has at least one component (a_j, v_j) with abscissa not in $\mathcal{R}_\varepsilon(A_i)$. So the energy-terms counted by $\mathsf{E}_k^+(\mathcal{R}_\varepsilon(A_i), V)$ all remain. We deduce that

$$\begin{aligned}\mathsf{E}_k^+(A_{i+1}, V) &= \mathsf{E}_k^+(\mathcal{R}_\varepsilon(A_i), V) \\ &\leqslant (1 - 2^{-k}\log(|A_i|)^{-1})\mathsf{E}_k^+(A_i, V) \\ &\leqslant (1 - 2^{-k}\log(|A|)^{-1})\mathsf{E}_k^+(A_i, V)\end{aligned}$$

for all $0 \leqslant i \leqslant I-1$.

Using the trivial bounds $|A||V| \leqslant \mathsf{E}_k^+(A, V) \leqslant |A|^k|V|$ we obtain the bound

$$(1-c_1)|A||V| \leqslant |A_I||V| \leqslant \mathsf{E}_k^+(A_I, V)$$

and similarly

$$\begin{aligned}\mathsf{E}_k^+(A_I, V) &\leqslant (1 - 2^{-k}\log(|A|)^{-1})\mathsf{E}_k^+(A_{I-1}, V) \\ &\leqslant (1 - 2^{-k}\log(|A|)^{-1})^I\mathsf{E}_k^+(A, V) \\ &\leqslant (1 - 2^{-k}\log(|A|)^{-1})^I|A|^k|V|\,.\end{aligned}$$

Thus we have the estimate

$$(1-c_1) < (1-2^{-k}\log(|A|)^{-1})^I |A|^{k-1} \leqslant e^{\frac{-c_1}{\varepsilon 2^k \log|A|}} |A|^{k-1} = e^{\frac{-c_1}{\varepsilon 2^k \log|A|} + \ln(2)(k-1)\log|A|}$$

Let us choose ε so that

$$(1-c_1) = e^{\frac{-c_1}{\varepsilon 2^k \log|A|} + \ln(2)(k-1)\log|A|}$$

to obtain a contradiction. That is, let us take

$$\varepsilon = \frac{c_1}{2^k \ln(2)(k-1)\log^2|A| - 2^k \log|A| \ln(1-c_1)}.$$

With this choice of ε, the process must terminate in at most $I = c_1\varepsilon^{-1}$ steps.

Having argued that this algorithmic procedure must indeed terminate after say $N \leqslant I$ steps, let us set $B = A_N$ and $C' = \mathcal{R}_\varepsilon(B)$. We have that $|B| \geqslant (1-c_1)|A|$. Set

$$C = \{x \in C' : r_{D_I+V}(a) \geqslant |\mathcal{P}_B|/(2^{k+1}|B|)\}.$$

Then

$$|\{(a,v) \in \mathcal{P}_B : a \in C' \setminus C\}| \leqslant \frac{|\mathcal{P}_B|}{2^{k+1}|B|}|C'| \leqslant \frac{|\mathcal{P}_B|}{2^{k+1}}.$$

Thus we obtain

$$|\{(a,v) \in \mathcal{P}_B : a \in C' \setminus C\}| \geqslant |G_N| - \frac{|\mathcal{P}_B|}{2^{k+1}} \geqslant \frac{|\mathcal{P}_B|}{2^k} - \frac{|\mathcal{P}_B|}{2^{k+1}} = \frac{|\mathcal{P}_B|}{2^{k+1}},$$

where the second inequality is a consequence of the termination condition.

On the other hand, since $C \subseteq C'$, recalling the definition of C', we have

$$|\{(a,v) \in \mathcal{P}_B : a \in C\}| \leqslant |C|\frac{|\mathcal{P}_B|}{\varepsilon|B|}.$$

Hence $|C| \geqslant \varepsilon 2^{-(k+1)}|B|$. With the explicit choice of ε together with the bound on $|B|$ this means that

$$|C| \geqslant \frac{c_1(1-c_1)}{2^{2k+1}\ln(2)(k-1)\log^2|A| - 2^{2k+1}\log|A|\ln(1-c_1)}|A| \geqslant \frac{c_1(1-c_1)}{2^{2k+1}\ln(2)(k-1)}\frac{|A|}{\log^2|A|}$$

Note that for any $c \in C$ we have

$$r_{P+V}(c) \in \left[\frac{|D_t|t}{2^{k+1}|B|}, \frac{2|D_t|t}{|B|}\frac{2^k\ln(2)(k-1)\log^2|A| - 2^k\log|A|\ln(1-c_1)}{c_1}\right].$$

The upper bound is certainly less than

$$\frac{2|D_t|t}{|B|}\frac{k2^k\log^2|A|}{c_1},$$

the bound that appears in the statement of the proposition. This completes the proof. □