

Sum-product inequalities with perturbation

*Dedicated to Mel Nathanson and Carl Pomerance
on the occasion of their 65th birthdays*

Spencer Backman

Ernie Croot

Mariah Hamel

Derrick Hart

April 30, 2010

1 Introduction

The standard sum-product inequality, as developed by Erdős and Szemerédi [4], and improved upon by Elekes [3], Ford [5], Nathanson [6], and Solymosi [8] [9], asserts that there exists some $\varepsilon > 0$ such that if A is a set of n real numbers (though Erdős and Szemerédi originally proved their theorem for $A \subseteq \mathbb{Z}$), then

$$|A + A| + |A.A| \geq n^{1+\varepsilon}, \text{ whenever } n > n_0. \quad (1)$$

There are various generalizations of this theorem to multiple sums and products, for example the following result of Bourgain and Chang [1]:

Theorem 1 (Bourgain-Chang) *For every $c > 0$ there exists $k \geq 1$ such that if S is a set of $n \geq 2$ rationals, then*

$$|kS| + |S^{(k)}| > n^c,$$

where kS denote the k -fold sumset $S + S + \cdots + S$, and $S^{(k)}$ denotes the k -fold product set $S.S...S$.

Though this is a truly marvelous theorem, it would be nice to have it hold for the *reals*, instead of just the *rationals*. One is tempted to try the following idea: Start with T as a set of n reals, and then approximate each element $t \in T$ by a rational s_t , and then let

$$S := \{s_t : t \in T\}$$

Bourgain-Chang will then show that either the k -fold sum or product set of S exceeds n^c (assuming all the s_t are distinct, which we will). But does that then mean the same must hold true for T , at least if one chooses the approximations carefully? Alas, the answer to this question is not obvious.

This problem of how robust sum-product theorems are under perturbation was partly what motivated the present paper, and we were able to prove a theorem in the case of a single sumset and product set (instead of k -fold ones, as in the Bourgain-Chang theorem). Now, of course, since we have sum-product theorems for the reals (in fact, the complex numbers) when a single sum and product are used, there is no need to bother with “perturbing” to the rational case; however, the theorem we prove is much more general than that.

In fact, our theorem is general enough so that we can easily deduce a “rounded sum-product theorem” as a corollary, which basically tells us that either the sumset $A + A$ is “small”; or else not only must $A.A$ be “large” (which we already get from previous sum-product theorems), but in fact the elements of the product set $A.A$ cannot “clump together too often”. The following is one such corollary:

Corollary 1 *Fix $0 < \varepsilon \leq 1$, and suppose that A is a set of n real numbers, all at least a distance 1 apart from each other. Then, if one lets R denote the elements of the product set $A.A$ rounded to the nearest multiple of $n^{1-\varepsilon}$, then*

$$|A + A| + |R| \gg n^{1+\varepsilon/9} / \log n.$$

To see what this is saying, suppose A is a subset of n numbers in $[1, 2n]$, all at least 1 apart from each other. Then, the product set lies in $[1, 4n^2]$, and there are $\sim 4n^{1+\varepsilon}$ multiples of the real number $n^{1-\varepsilon}$ in this interval. The corollary here is telling us that $\gg n^{1+\varepsilon/9} / \log n$ of these multiples must be “near” to an element of $A.A$.

The proof of this corollary is discussed after the remarks following Theorem 2 in the next section.

One wonders whether these types of ideas (sum-product inequalities with perturbation) can somehow be used to improve upon the results of Balog [2] on smooth numbers. Attempting such a feat with sum-product technology was another, hidden motivation behind the present paper, though the results we have developed so far are much too weak to say anything interesting on smooth numbers.

2 The Main Theorem

It is interesting to consider whether one can prove a finer version of (1), where one is allowed to “perturb” the products $ab \in A$ a little bit: suppose that for each pair $a, b \in A$ we get to choose “perturbation parameters” $\delta_{a,b}$ and $\delta'_{a,b}$, where say

$$\delta_{a,b}, \delta'_{a,b} \in [-1, 1].$$

Given these parameters, define the “perturbed product set”

$$P := \{(a + \delta_{a,b})(b + \delta'_{a,b}) : a, b \in A\}.$$

Must it be the case that for all choices of $\delta_{a,b}, \delta'_{a,b}$ we get that

$$|A + A| + |P| \geq n^{1+\varepsilon} ?$$

The answer is obviously ‘no’, since if the elements of A are close enough together, and are in arithmetic progression, we can easily choose $\delta_{a,b}$ and $\delta'_{a,b}$ so that

$$|A + A| + |P| = 2n.$$

But what if we add the condition that the elements of A are all spaced at least 1 apart? Can we show that $|A + A| + |P|$ must always be large?

Again the answer is ‘no’, but the natural example is a little more complicated. Basically, consider the arithmetic progression

$$A := \{x + 1, x + 2, \dots, x + n\}. \tag{2}$$

This set has the property that it is “close” to the geometric progression

$$\{x(1 + 1/x)^j : j = 0, 1, \dots, n - 1\}. \tag{3}$$

Indeed,

$$x(1 + 1/x)^j = x + j + O(j^2/x),$$

for $x \geq n$. So, clearly, for x big enough relative to n we will have that if the $\delta_{a,b}, \delta'_{a,b}$ are allowed to vary over $[-1, 1]$, we can force

$$P = A + A,$$

thereby making

$$|A + A| + |P| \leq 4n - 2.$$

But we can give even better upper bounds on $\delta_{a,b}$ and $\delta'_{a,b}$ that make $|P| + |A + A|$ small: first, set all $\delta'_{a,b} = 0$. Then suppose that a and b correspond to the numbers (3) using exponents j and k , respectively. Next, we choose $\delta_{a,b} \ll n/x$ so that

$$\begin{aligned} (a + \delta_{a,b})b &= x^2(1 + j/x + O(j^2/x^2) + \delta_{a,b})(1 + k/x + O(k^2/x^2)) \\ &= x^2(1 + (j + k)/x + \delta_{a,b} + O(n^2/x^2)). \end{aligned}$$

So, if $\delta_{a,b}$ is the negative of this $O(n^2/x^2) < O(n/x)$, then the product will be just $x^2(1 + (j + k)/x)$, meaning that we can make our perturbed product set into an arithmetic progression, making $|P| + |A + A| \ll n$.

So, to achieve a lower bound on $|P| + |A + A|$ that is substantially better than the trivial bound, we will need that $\delta_{a,b}, \delta'_{a,b}$ can only vary over intervals that are width $O(n/x)$. Our main theorem below will show that this is essentially best possible, as the intervals for $\delta_{a,b}$ and $\delta'_{a,b}$ leading to non-trivial results will have lengths $n^{1-\varepsilon}/a$ and $n^{1-\varepsilon}/b$, respectively. Actually, our theorem is even more general, since following Remark 2 at the end of our theorem, the sumset $A + A$ can also be perturbed, and still we get a good lower bound on the resulting perturbed sum and product sets.

Our main theorem is as follows:

Theorem 2 *Suppose $0 < \varepsilon \leq 1$ and let A be a set of $n > n_0(\varepsilon)$ positive real numbers, all at least 1 apart. For each pair $(a, b) \in A \times A$, suppose that $\delta_{a,b}$ and $\delta'_{a,b}$ are arbitrary real numbers satisfying*

$$|\delta_{a,b}| < \frac{n^{1-\varepsilon}}{a}, \text{ and } |\delta'_{a,b}| < \frac{n^{1-\varepsilon}}{b}. \quad (4)$$

Finally, define the perturbed product set

$$P := \{(a + \delta_{a,b})(b + \delta'_{a,b}) : a, b \in A\}.$$

Then, we have that

$$|P| + |A + A| \gg \frac{n^{1+\varepsilon/9}}{\log n}.$$

Remark 1. Obviously, if the elements of A are not at least 1 apart, we can rescale to make it true. Furthermore, all we really need is that the median of the gaps between consecutive elements of A is at least 1, since by deleting at most $n/2$ elements from A we get a set of elements that are all at least 1 apart.

Remark 2. From the proof one can show that if we also perturb the sums $A + A$, we have the same quality lower bound on the sums and products; that is, suppose we define S to be the set of all perturbed sums $a + b + \delta''_{a,b}$, where $|\delta''_{a,b}| \leq n^{1-\varepsilon}/(a+b)$. Then, we can show

$$|P| + |S| \gg \frac{n^{1+\varepsilon/9}}{\log n}. \quad (5)$$

See remarks at the end of the proof of Theorem 2 for a discussion of how this is proved.

Proof of Corollary 1. Given a pair $a, b \in A$ with $a \leq b$, we let $\delta'_{a,b} = 0$ and then we select $\delta_{a,b}$ so that

$$(a + \delta_{a,b})(b + \delta'_{a,b}) = (a + \delta_{a,b})b$$

is the nearest multiple of $n^{1-\varepsilon}$ to ab . It is possible to choose such $\delta_{a,b}$, since this only requires

$$|\delta_{a,b}| < n^{1-\varepsilon}/b,$$

which is smaller than the upper bound of $n^{1-\varepsilon}/a$ that we are allowed. \blacksquare

3 Proof of Theorem 2

3.1 Preliminaries

We will basically follow a variant of Elekes's original argument used to prove that if A is a set of n reals, then

$$|A + A| \cdot |A.A| \gg n^{5/2},$$

from which it follows that

$$|A + A| + |A.A| \gg n^{5/4}.$$

But our approach will differ in that the Szemerédi-Trotter theorem [11] is not directly amenable to our particular approach. Instead, we apply a very minor generalization of the Szemerédi-Trotter curve theorem of Székely [10] (hardly any generalization at all), which follows by the same proof as that of Székely.

Theorem 3 *Suppose that one has a collection of ℓ non-self-crossing curves and p points. Let C denote the collections of curves. Let m_1 denote the maximum over all pairs of points p_1, p_2 , of the number of curves that are incident to both p_1 and p_2 , that pass through any given pair of points p_1, p_2 , and let m_2 denote the “average intersection multiplicity”, defined as follows*

$$m_2 := \binom{\ell}{2}^{-1} \sum_{\{c_1, c_2\} \subseteq C} |c_1 \cap c_2|.$$

Then, the number of incidences I , which is the number of point-curve pairs, where the point is on the curve, satisfies

$$I \ll (m_1 m_2)^{1/3} (p\ell)^{2/3} + \ell + m_1 p.$$

The way this differs from the Szemerédi-Trotter curve theorem in [10] is that m_2 is the *average* intersection multiplicity among the curves, not an absolute upper limit on the intersection multiplicity between pairs of curves.

The proof of Székely begins with the following result on the crossing number $\text{cr}(G)$ of a multigraph G , as appears in [10, Theorem 7].

Theorem 4 *Suppose that G is a multigraph with p nodes, e edges and edge multiplicity m . Then, either $e < 5pm$ or $\text{cr}(G) \geq ce^3/(p^2m)$.*

Proof of Theorem 3. Now to prove Theorem 3 we construct a graph as follows: fix one of our ℓ curves, and consider which of our p points happens to lie on it. By choosing a direction with which to traverse the curve, we create an ordering of these incident points. If there are x such points on the given curve, then we form $x - 1$ curve segments that adjoin consecutive pairs of points. We throw away the “infinite parts” of the curves as they will play no further role in our proof.

Letting I denote our total number of incidences, and e the number of edges in our graph, we will have

$$e = I - \ell,$$

since the number of edges each curve contributes is one less than its number of incident points. Letting C denote our set of curves, we also have that

$$\text{cr}(G) \leq \sum_{\{c_1, c_2\} \subset C} |c_1 \cap c_2| = \binom{\ell}{2} m_2.$$

Finally, note that in our drawing of the graph $m = m_1$.

Putting all this together, we either have that $e < 5m_1p$, which would imply

$$I = e + \ell < 5m_1p + \ell,$$

which implies our theorem, or else

$$(I - \ell)^3 / (p^2 m_1) = e^3 / (p^2 m_1) \ll \text{cr}(G) \leq \binom{\ell}{2} m_2.$$

Theorem 3 is now proved. ■

3.2 Restricting to a dyadic interval

Later, we will require an upper bound on the number of curves passing through pairs of grid points, and to achieve such upper bounds it will be good to first pass to elements of A that lie in a dyadic interval. To this end we will require the following lemma.

Lemma 1 *Suppose that A is a set of n real numbers satisfying $|A + A| \leq n^{1+\delta}/3 \log n$, for some $\delta > 0$. Then, there exists a dyadic interval $[x, 2x)$ containing at least $n^{1-\delta}$ elements of A .*

A version of this lemma can be proved without too much trouble using only very elementary ideas; however, we give a proof using the Ruzsa-Plünnecke inequality, since it makes the proof short and transparent. First, let us state the Ruzsa-Plünnecke inequality [7].

Theorem 5 *Suppose that A is a subset of an additive abelian group, such that*

$$|A + A| \leq K|A|.$$

Then,

$$|kA - \ell A| = |A + A + \cdots + A - A - A - \cdots - A| \leq K^{k+\ell}|A|.$$

Proof of Lemma 1. Suppose, for proof by contraposition, that every dyadic interval contains fewer than $n^{1-\delta}$ elements of A . Then, it requires at least n^δ disjoint dyadic intervals to contain all the elements of A , and therefore choosing one element from every other dyadic interval (if these disjoint dyadic intervals are put into increasing order), we get a sequence of at least $n^\delta/2$ elements

$$A' := \{a_1, \dots, a_h\} \subseteq A, \quad h \geq n^\delta/2,$$

such that

$$a_{i+1}/a_i \geq 2.$$

It is a simple matter to show that all the k -fold sums of distinct elements of A' are distinct (think about the usual proof that binary number representations are unique); and so, if we assume that $|A + A| = K|A|$, then from Theorem 5

$$(n^\delta/k)^k \leq \binom{n^\delta/2}{k} < |kA'| \leq |kA| \leq K^k n.$$

It follows that

$$K \geq n^{\delta-1/k}/k.$$

Choosing $k \sim \log n$ we get that

$$K > n^\delta/3 \log n.$$

But this means that

$$|A + A| = Kn > n^{1+\delta}/3 \log n,$$

so the lemma is proved. ■

Now we choose the dyadic interval $[x, 2x)$ containing the most elements of A . We may assume that this interval contains at least $n^{1-\kappa\varepsilon}$ elements of A , where we define the constant

$$\kappa = 1/9,$$

since otherwise Lemma 1, with $\delta = \kappa\varepsilon$ implies that $|A + A| > n^{1+\kappa\varepsilon}/3 \log n$, thereby proving Theorem 2.

Let B denote those $\geq n^{1-\kappa\varepsilon}$ elements of A contained in $[x, 2x)$. We note that if we consider the products

$$(a + \delta_{a,b})(b + \delta'_{a,b}), \quad a, b \in B,$$

then as we vary over all legal choices for $\delta_{a,b}$ and $\delta'_{a,b}$, since a and b lie in the same dyadic interval $[x, 2x)$, we have that the possible values of this product must lie in an interval of width

$$\ll n^{1-\varepsilon} + n^{2-2\varepsilon}/x^2.$$

Since the gap between elements of A is at least 1, we have $x \gg n$, making our interval of width

$$\ll \Delta := n^{1-\varepsilon}.$$

So, the number of our “perturbed products” is at least a constant multiple of the set of distinct values $\langle ab \rangle$, $a, b \in B$, where $\langle t \rangle$ denotes t rounded to the nearest multiple of Δ .

3.3 A family of polygonal curves

In order to apply Theorem 3, we need to define some points and curves that are relevant to our problem: we begin by letting X be the elements of $B + B$; and then we let Y be the elements of $B \cdot B$ rounded to the nearest multiple of Δ . Our set of points will then be $X \times Y$; so, there will be $|X| \cdot |Y|$ of them in total.

Now we define the curves: we begin by considering, for each $a, b \in B$, the set of points on the line

$$y = a(x - b),$$

with $x \in B + b$. Then, we round the y coordinate to the nearest multiple of Δ . Sweeping from left-to-right across the grid, we connect consecutive points by line segments.

3.4 Perturbing the curves

At this point we could have that some pairs of curves intersect in a segment, and therefore have infinitely many points of intersection. But this is easily fixed by making a small perturbation to the curves, replacing the shared segments by closely drawn curves that are nearly parallel and only intersect

at grid points. We furthermore can assume that if a pair of points is common to two or more curves, then those points must be grid points (again, by perturbing the curves slightly, while still connecting the same grid points as before).

3.5 The average crossing number

Now we calculate the average intersection multiplicity of pairs of curves: first, we observe that the polygonal curves are at most a vertical distance Δ from their corresponding straight lines. And therefore, two of these polygonal curves, corresponding, say, to the curves

$$y = a(x - b) \text{ and } y = c(x - d),$$

can only cross if x is such that

$$|c(x - d) - a(x - b)| < \Delta.$$

In other words,

$$|(c - a)x + ab - cd| < n^{1-\varepsilon}.$$

We first consider the contribution to our count of the average intersection multiplicity of all those pairs of lines having the same slope: in order for the polygonal curves corresponding to lines of the same slope to intersect, they must have y -intercepts that come within Δ of one another, and when this happens we will just assume that the lines intersect in $|B|$ points, the maximum possible. Since there are $|B|^4$ choices for $(a, b, c, d) \in B^4$, the contribution to our average intersection multiplicity count of pairs of lines of the same slope is

$$\ll \frac{1}{|B|^4} \sum_{\substack{a, b, b' \in B \\ |b - b'| \leq \Delta}} |B| \leq 1.$$

Note that we just used here the trivial bound – we didn't even need to use the fact that $|b - b'| \leq \Delta$.

Next, we consider the contribution of pairs of lines that have different slope. We begin by observing that between any consecutive x -values of the set

$$\{b, d\} + B, \tag{6}$$

there can be at most one crossing between the pair of polygonal curves.

Now, since in any three consecutive points of (6), two must either belong to $b + B$ or to $d + B$, we have that every other point of (6) is at least 1 apart. It follows, therefore, that the number of crossings between the two polygonal curves is at most

$$1 + O(n^{1-\varepsilon}/(c-a)).$$

(The 1 here accounts for the “left-most point of intersection”, and once we are given this point, there can be at most $O(n^{1-\varepsilon}/(c-a))$ other intersection points to the right of it.) Thus, the average intersection multiplicity, is easily seen to be bounded from above by

$$\begin{aligned} 1 + \frac{O(n^{1-\varepsilon})}{|B|^2} \sum_{\substack{a, c \in B \\ c > a}} \frac{1}{c-a} &\leq 1 + \frac{O(}{n^{1+\varepsilon(1-\kappa)})} \sum_{1 \leq i < j \leq n} \frac{1}{(j-i)} \\ &\leq 1 + \frac{O(\log n)}{n^{\varepsilon(1-\kappa)}}. \end{aligned}$$

So, the average intersection multiplicity is bounded from above by a function that is $O(1)$; that is,

$$m_2 \ll 1. \tag{7}$$

3.6 The number of curves meeting in a pair of points

Next, we need to produce an upper bound on the number of curves that can meet in a pair of points. We begin by noting, by the way we perturbed the curves in subsection 3.4, that in order for two or more curves to meet in a pair of points, those points must both be elements of $B + B$; furthermore, if any of such curves corresponds, say, to a line $y = a(x - b)$, then that pair of points must lie in $B + b$. And so, the pair of points must be at least 1 apart.

It is easy to see, then, that the curves meeting in a pair of points, $(x_1, y_1), (x_2, y_2)$, $x_2 > x_1 + 1$, are at most in number the set of lines of the form

$$f_i(x) = a_i(x - b_i),$$

where all the $f_i(x_1)$ come within Δ of one another, and the same should hold for $f_i(x_2)$. But this implies that

$$|(a_i - a_j)(x_1 - x_2)| \leq 2\Delta. \tag{8}$$

First, let us see that no two of these lines can have the same slope: if they did, say $a_i = a_j$, then just considering the contribution of the point with

$x = x_1$, we would have that

$$a_i(x_1 - b_i) = a_j(x_1 - b_j),$$

and therefore $b_i = b_j$. But this can only hold if the two lines are in fact the same, so we may assume the slopes are different. Assuming this, we find from (8) that

$$|a_i - a_j| \leq 2\Delta = 2n^{1-\varepsilon}.$$

It is clear that, since the $a_i \in B$ are all at least 1 apart, there can be at most $O(n^{1-\varepsilon})$ choices for the slopes a_i such that all pairwise differences $|a_i - a_j|$ satisfy this bound.

We have therefore proved that

$$m_1 \ll n^{1-\varepsilon}. \quad (9)$$

Here we are assuming that $\varepsilon \leq 1$, because of course we know that $m_1 \geq 1$.

3.7 Conclusion of the proof

Putting everything together, since our $|B|^2 = n^{2-2\kappa\varepsilon}$ lines hit the grid $X \times Y$ in $|B| = n^{1-\kappa\varepsilon}$ points each, we have that the number of incidences is $n^{3-3\kappa\varepsilon}$. Yet, from Theorem 3, along with (7) and (9), we find that the number of incidences is

$$\ll (m_1 m_2)^{1/3} (|X| \cdot |Y| \cdot n^{2-2\kappa\varepsilon})^{2/3} \ll n^{1/3-\varepsilon/3} (|X| \cdot |Y| \cdot n^{2-2\kappa\varepsilon})^{2/3}.$$

So,

$$|X| \cdot |Y| \gg n^{2-\varepsilon(5\kappa/2-1/2)}$$

So,

$$|X| + |Y| \gg n^{1+\varepsilon(1/4-5\kappa/4)} \gg n^{1+\varepsilon/9}.$$

Note that here is where we used the fact that ε is sufficiently small – it allowed us to ignore the contribution of the terms $\ell + m_1 p$.

This completes the proof.

We conclude this section by giving some remarks about how to prove (5): basically, the reason we can show this is that in the first parts of the proof of Theorem 2 above, we pass to a subset $B \subseteq A$, contained in a dyadic interval $[x, 2x)$, whose set of perturbed products or sums $B+B$ we show must contain

at least $n^{1+\varepsilon/9}/3 \log n$ elements. This then means that $|\delta''_{a,b}| < n^{1-\varepsilon}/x$; and, then we can bound $|S|$ from below by a constant multiple of $|C + C|$, where C is the set of elements of B rounded to the nearest multiple of $n^{1-\varepsilon}/x$. Rewriting the perturbed products for B in terms of perturbed products for C , it is easy to see that this implies (5).

References

- [1] J. Bourgain and M.-C. Chang, *On the size of k -fold sum and product sets of integers*, J. Amer. Math. Soc. **17** (2004), 473-497.
- [2] A. Balog, *On the distribution of integers having no large prime factor*, Journées Arithmétiques, Besançon, Astérisque **147/148** (1985), 27-31.
- [3] G. Elekes, *On the number of sums and products*, Acta Arith. **81** (1997), 365-367.
- [4] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics; To the memory of Paul Turán, P. Erdős, L. Alpar, and G. Halasz, editors. Akadémiai Kiado-Birkhauser Verlag, Budapest-Basel-Boston, Mass. 1983, 213-218.
- [5] K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan Jour. **2** (1998), 59-66.
- [6] M. Nathanson, *On sums and products of integers*, Proc. Amer. Math. Soc. **125** (1997), 9-16.
- [7] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97-109.
- [8] J. Solymosi, *On sum-sets and product sets of complex numbers*, J. Th. Nomb. Bordeaux **17** (2005), 921-924.
- [9] ———, *An upper bound on the multiplicative energy*, preprint on the ARXIVES.
- [10] A. Székely, *Crossing numbers and hard Erdős problems in discrete geometry*, Comb. Prob. and Comp. **6** (1997), 353-358.

- [11] E. Szemerédi and W. Trotter, *Extremal problems in discrete geometry*,
Combinatorica **3** (1983), 381-392.