SUM-PRODUCT Theorems
An Exposition by William Gasarch

1 Introduction

Let A be a set of n reals.

Def 1.1

$A + A = \{x + y : x, y \in A\}$

$A \cdot A = \{xy : x, y \in A\}$

$A/A = \{x/y : x, y \in A\}$ (This one assumes $0 \notin A$.)

We will show the following.

- At least one of $|A + A|$ or $|A \cdot A|$ is "large". (These are called "Sum-Product Theorems".)
- At least one of $|A + A|$ or $|A/A|$ is "large".

We were inspired to do this exposition by Avi Wigderson's applications of sum-product theorems [16].

Example 1.2 $A = \{1, 2, \ldots, n\}$. Then

- $A + A = \{2, \ldots, 2n\}$, so $|A + A| = O(n)$.
- $A \cdot A = \{xy \mid x, y \in [n]\}$. For a rough estimate just consider the primes in $\{2, \ldots, n\}$. There are $\Theta(n/\log n)$ of them. Each product of two primes is unique, hence $|A \cdot A| \geq \Omega(n^2/(\log n)^2)$.
- $A/A = \{x/y \mid x, y \in [n]\}$. For a rough estimate just consider the primes in $\{2, \ldots, n\}$. There are $\Theta(n/\log n)$ of them. Each product of two primes is unique, hence $|A/A| \geq \Omega(n^2/(\log n)^2)$.

Example 1.3 $A = \{2^1, 2^2, \ldots, 2^n\}$. Then

- $A + A$. The sums are all of the form $2^a + 2^b$. We claim that if $2^a + 2^b = 2^c + 2^d$ then $\{a, b\} = \{c, d\}$; hence $|A + A| = \Omega(n^2)$. Assume

$$2^a + 2^b = 2^c + 2^d.$$

We can assume that $a = \min\{a, b, c, d\}$. Divide by 2^a to obtain

$$1 + 2^{b-a} = 2^{c-a} + 2^{d-a}.$$

By a parity argument an odd number of $b-a$, $c-a$ and $d-a$ are 0. We consider the cases.

1. $a = b$. Then we have
$$2 = 2^{c-a} + 2^{d-a}.$$
We must have $a = c$ and $a = d$. So $a = b = c = d$, hence $\{a, b\} = \{c, d\}$.
2. $a = c$. Then we have
$$1 + 2^{b-a} = 1 + 2^{d-a}, \text{ and}$$
$$2^{b-a} = 2^{d-a}.$$
So $b - a = d - a$, so $b = d$. Hence $\{a, b\} = \{c, d\}$.
3. $a = d$. Then we have
$$1 + 2^{b-a} = 2^{c-a}1.$$
$$2^{b-a} = 2^{c-a}.$$
$$b - a = c - a$$
$b = c$. Hence $\{a, b\} = \{c, d\}$.
4. $a = b$ and $c = a$ and $d = a$. So $a = b = c = d$, hence $\{a, b\} = \{c, d\}$.

- $A \cdot A = \{2^2, \ldots, 2^{2n}\}$, so $|A \cdot A| = O(n)$.
- $A/A = \{2^{-n}, \ldots, 2^n\}$, so $|A/A| = O(n)$.

Note that in both examples either $|A + A|$ or $|A \cdot A|$ was large. There have been many theorems that say that at least one of them is large. We list theorems about these concepts and then prove two of them. We will prove the two strongest theorems known about one of $|A \cdot A|$ and $|A + A|$ being large for A a finite set of reals. We will then obtain a result about $|A + A|$ or $|A/A|$ being large using the machinery of the second result.

1. Erdös and Szemerédi [14] showed that there exists a constant ϵ such that if A is a set of n integers then
$$\max\{|A + A|, |A \cdot A|\} = \Omega(n^{1+\epsilon}).$$
2. Nathanson [8] showed that if A is a set of n integers then
$$\max\{|A + A|, |A \cdot A|\} = \Omega(n^{1+(1/31)}).$$
3. Chen [4] showed that if A is a set of n integers then
$$\max\{|A + A|, |A \cdot A|\} = \Omega(n^{1+(1/20)}).$$

4. Ford [6] showed that if A is a set of n integers then

$$\max\{|A+A|, |A \cdot A|\} = \Omega(n^{1+(1/15)}).$$

5. Elekis [5]) showed that if A is a set of n reals then

$$\max\{|A+A|, |A \cdot A|\} = \Omega(n^{1+(1/4)}).$$

   We will present a proof of this theorem.

6. Solymosi [11] (see also [15] showed that if A is a set of n reals then

$$\max\{|A+A|, |A \cdot A|\} = \Omega\Big(\frac{n^{1+(3/11)}}{(\log n)^{3/11}}\Big).$$

   We will present a proof of this theorem. Our source is [15].

7. Bourgain, Katz, Tao [2] investigated sum-product theorems over the finite fields of order p. They showed the following: There exists a functions $c : (0,1) \to \mathrm{R}^{>}0$ and $\epsilon : (0,1) \to (0,1)$ such that the following is true. Let p be a prime and F_p is the field on p elements. Let $\delta \in (0, 1/2)$. If $A \subseteq F_p$ and $p^\delta < |A| < p^{1-\delta}$ then

$$\max\{|A+A|, |A \cdot A|\} \geq c(\delta)|A|^{1+\epsilon(\delta)}.$$

8. LOOK INTO THIS LATER there exists an absolute constant c such that the following is true. Let p be a prime. Let A be a subset F_p (the field of p elements) of size n. Let $k \geq 1$ be such that there is no finite subfield G of F of cardinality $|G| \leq k|A|$ and no $x \in F$ such that $|A-(x \cdot G)| \leq k$. Then either $|A| = O(k^{O(1)})$ or

$$\max\{|A+A|, |A \cdot A|\} = \Omega(k^c|A|).$$

   For proof see the reference above or [15].

9. Solymosi [11] (see also [15]) showed that if A is a set of n complex numbers then

$$\max\{|A+A|, |A \cdot A|\} = \Omega(n^{1+(1/4)}).$$

10. M. Chang [3] showed the following two theorems.

    (a) There exists a function $\Phi(n)$ which goes to infinity such that the following is true. Let d be a fixed integer. Let A be a finite set of n $d \times d$ real matrices such that, for all M, M' distinct elements of the set, $det(M - M') \neq 0$. Then

$$\max\{|A+A|, |A \cdot A|\} = \Omega(n\Phi(n)).$$

(b) For every d there exists $\epsilon > 0$ such that the following holds. Let A be a set of n $d \times d$ real symmetric matrices. Then

$$\max\{|A + A|, |A \cdot A|\} = \Omega(n^{1+\epsilon}).$$

The proofs we present depend on the Szemerédi-Trotter theorem. The proof of the Szemerédi-Trotter theorem that we present depends on the Crossing Lemma. Hence we prove the Crossing Lemma and then the Szemerédi-Trotter theorem. Both of these results are interesting in their own right and have many other applications.

2 The Crossing Lemma

The following is well known and easy to find, so we will not prove it.

Lemma 2.1 *If $G = (V, E)$ is a planar graph with v vertices and e edges then $e \leq 3v - 6$.*

Def 2.2 Let G be a graph. The *crossing number* of G is the minimal number of non-vertex crossings that the graph can be drawn with. We often denote the crossing number by c. Note that a planar graph has crossing number 0.

Lemma 2.3 *If $G = (V, E)$ is a graph with v vertices, e edges, and crossing number c then $c \geq e - 3v$.*

Proof:

First draw the graph in the plane with c non-vertex crossings. Remove the edges that cause the crossings one at a time until the graph is planar. The new graph G' has v vertices and $e - c$ edges. By the prior lemma

$$e - c \leq 3v - 6$$

$$e \leq 3v + c - 6.$$

$$c \geq e - 3v + 6 \geq e - 3v.$$

∎

We will get a much better lower bound on c. This result, called *The Crossing Lemma*, was proven independently by Ajtai, Chvátal, Newborn, Szemerédi [1] and Leighton [7].

Lemma 2.4 *Let $G = (V, E)$ be a graph with v vertices's, e edges, and crossing number c. If $e \geq 4v$ then $c \geq \Omega(\frac{e^3}{v^2})$.*

Proof: Let p be a probability that we will set later. For every vertex in the graph remove it with probability $1-p$. Let the resulting graph be $G = (V', E')$. We denote the number of vertices by v', the number of edges by e', and the crossing number by c'.

$E(v') = vp$ since we retain each edge with probability p.

$E(e') = ep^2$ since we need to retain both of the endpoints to retain the edge.

$E(c') \leq cp^4$ since if you retain all four vertices then you might retain the crossing, but if you lose any one of them then you won't.

By Lemma 2.3 we have

$$c' \geq e' - 3v'.$$

By the linearity of expectation we have

$$E(c') \geq E(e') - 3E(v')$$

Combining this with what we already know about $E(v')$, $E(e')$ and $E(c')$ we obtain

$$cp^4 \geq E(c') \geq ep^2 - 3vp.$$

$$c \geq \frac{e}{p^2} - \frac{3v}{p^3}.$$

Set $p = 4v/e$ (this is where we use $e > 4v$).

Then we get

$$c \geq \frac{e^3}{64v^2} = \Omega\Big(\frac{e^3}{v^2}\Big).$$

∎

Note 2.5 The hypothesis $e \geq 4v$ of Lemma 2.4 can be weakened to $e \geq (3+\epsilon)v$ for any $\epsilon > 0$.

Note 2.6 The above proof gives $c \geq \frac{e^3}{64v^2} \sim 0.0156\frac{e^3}{v^2}$. The best result known to date is by Pach, Radoicic, Tardos, and Toth [10] who have that if $e \geq 7n$ then $c \geq 0.032\frac{e^3}{v^2}$. It is know that there are an infinite number of n such that there is a graph on n vertices with graphs with $e \geq 7n$ and $c \leq 0.09\frac{e^3}{v^2}$.

3 The Szemerédi-Trotter Theorem

If you have a set of points P, and a set of lines L, how many times do a point and a line meet? They could of course meet 0 times. What is the maximum amount of times they could meet?

Def 3.1 Let P be a set of points and L be a set of lines. An *incidence of P and L* is a pair $(p, \ell) \in P \times L$ such that point p is on line ℓ. Let

$$I_{P,L} = \{(p, \ell) : p \in P, \ell \in L \text{ and } p \text{ is on } \ell\}.$$

We will leave out the subscripts if they are understood.

We will prove the following theorem:

$$|I| = O(|P| + |L| + (|L||P|)^{2/3}).$$

This was first proven by Szemerédi and Trotter [13]. Different proofs can be found in [9]. We present the simplest known proof, due to Székely [12].

Theorem 3.2 *For any set of P points and L lines in the plane,*

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

Proof:

Define a graph $G = (V, E)$ as follows:
$V = P$, the set of points.
$E = \{(x, y) : \ x \text{ and } y \text{ are both on some line } \ell \in L \text{ and are adjacent } \}$.

Let $v = |V|$ and $e = |E|$. It is easy to see that $v = P$ The number of edges is harder to determine. Let the lines be $\ell_1, \ell_2, \ldots, \ell_L$. Assume that ℓ_i has p_i points of P on it. Then ℓ_i is responsible for $p_i - 1$ edges. Hence the total number of edges is

$$\sum_{i=1}^{|L|}(p_i - 1) = (\sum_{i=1}^{|L|} p_i) - |L| = |I| - |L|.$$

Hence

$$e = |I| - |L|.$$

Look at the natural way to draw the graph— placing the points where they are naturally. Where there is a crossing you must have two of the lines intersecting. Hence there are at most $|L|^2$ crossings. Hence

$$c \leq |L|^2.$$

We want to apply Lemma 2.4. However, for this we need $e \geq 4v$. But this might not be true. Hence we have two cases.
Case 1: $e < 4v$. Hence $|I|-|L| \leq 4|P|$, so $|I| \leq 4|P|+|L| = O(|P|+|L|+(|L||P|)^{2/3})$.

Case 2: $e \geq 4v$. We apply Lemma 2.4 to obtain

$$|L|^2 \geq c \geq \Omega\Big(\frac{e^3}{v^2}\Big) = \Omega\Big(\frac{(|I|-|L|)^3}{|P|^2}\Big)$$

$$(|L||P|)^2 \geq \Omega((|I|-|L|)^3)$$

$$(|L||P|)^{2/3} \geq \Omega(|I|-|L|)$$

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

∎

Note 3.3 The best known upper and lower bounds on I are due to Pach, Radoicic, Tardos, and Toth [10], They are

$$0.42(|L||P|)^{2/3}+|L|+|P| \leq |I| \leq 2.5(|L||P|)^{2/3}+|L|+|P|.$$

4 Corollaries of the Szemerédi-Trotter Theorem

We state two corollaries that we will need in the second product-sum theorem.

Lemma 4.1 *Let P be a set of points and let $k \in \mathsf{N}$. (We assume k is bigger than any constant we may encounter.) Let*

$$L = \{\ell : \ell \text{ has at least } k \text{ points from } P \text{ on it}\}.$$

Then

$$|L| = O\Big(\max\Big\{\frac{|P|}{k}, \frac{|P|^2}{k^3}\Big\}\Big).$$

Proof: Note that the number of incidences of P and L is at least $k|L|$. Hence

$$|I| \geq k|L|.$$

Using this and Theorem 3.2 to P and L to obtain

$$k|L| \leq |I| \leq O(|P|+|L|+(|L||P|)^{2/3}).$$

There are two cases.

Case 1: $(|L||P|)^{2/3} \leq |P| + |L|$.

$$k|L| \leq O(|P| + |L|) \leq O(|P|) + O(|L|)$$

$$|L| \leq O\Big(\frac{|P|}{k}\Big).$$

Case 2: $|P| + |L| \leq (|L||P|)^{2/3}$.

$$k|L| \leq O(|L||P|)^{2/3})$$

$$k|L|^{1/3} \leq O(|P|^{2/3})$$

$$k^3|L| \leq O(|P|^2)$$

$$|L| \leq O\Big(\frac{|P|^2}{k^3}\Big)$$

Combining the two cases yields

$$|L| = O\Big(\max\Big\{\frac{|P|}{k}, \frac{|P|^2}{k^3}\Big\}\Big).$$

∎

Lemma 4.2 *Let L be a set of lines and let $k \in \mathsf{N}$. Let*

$$P = \{p : p \text{ is on at least } k \text{ lines from } L\}.$$

Then

$$|P| = O\Big(\max\Big\{\frac{|L|}{k}, \frac{|L|^2}{k^3}\Big\}\Big).$$

Proof: Note that the number of incidences of P and L is at least $k|P|$. Hence

$$|I| \geq k|P|.$$

Using this and Theorem 3.2 to P and L to obtain

$$k|P| \leq |I| \leq O(|P| + |L| + (|L||P|)^{2/3}).$$

There are two cases.

Case 1: $(|L||P|)^{2/3} \leq |P| + |L|$.

$$k|P| \leq O(|P| + |L|)$$

$$|P| \leq O\Big(\frac{|L|}{k}\Big).$$

Case 2: $|P| + |L| \leq (|L||P|)^{2/3}$.

$$k|P| \leq O((|L||P|)^{2/3})$$

$$k|P|^{1/3} \leq O(|L|^{2/3})$$

$$k^3|P| \leq O(|L|^2)$$

$$|P| \leq O\Big(\frac{|L|^2}{k^3}\Big)$$

Combining the two cases results in

$$|P| = O\Big(\max\Big\{\frac{|L|}{k}, \frac{|L|^2}{k^3}\Big\}\Big).$$

∎

5 The $n^{1+(1/4)}$-Product-Sum Theorem

Elekis [5] showed the following theorem.

Theorem 5.1 *If A is a set of n reals then*

$$\max\{|A+A|, |A \cdot A|\} = \Omega(|A|^{1+(1/4)}).$$

Proof:

Let $P = (A+A) \times (A \cdot A)$. Let $s = |A+A|$ and $p = |A \cdot A|$. Note that $|P| = sp$. We will show that $sp \geq \Omega(n^{5/2})$, hence one of s, p has to be $\geq \Omega(n^{5/4})$.

Let L be the set of lines of the form $y = x/a + a'$ where $a, a' \in A$. Note that $|L| = |A|^2$.

How many incidences are there? Let $y = x/a + a'$ be a line in L. Note that for all $a'' \in A$ the point $(aa'', a' + a'') \in P$ is on the line. Hence each line has at least $|A|$ incidences. Therefore there are at least $|A|^3$ incidences.

Combining this with Theorem 3.2 we obtain

$$|A|^3 \leq |I| \leq O(|A|^2 + sp + (|A|^2 sp)^{2/3}).$$

Hence

$$|A|^3 \leq O(sp + (|A|^2 sp)^{2/3})$$

Assume, by contradiction, that $sp << |A|^{5/2}$. Then

$$|A|^3 \leq O(sp + (|A|^2 sp)^{2/3}) << O(|A|^{5/2} + (|A|^{9/2})^{2/3}) \leq O(|A|^3).$$

This is a contradiction. Hence $sp \geq \Omega(|A|^{5/2})$. Therefore

$$\max\{|A+A|, |A \cdot A|\} = \Omega(|A|^{5/4}).$$

∎

6 The $n^{(1+3/11)}/(\log n)^{3/11}$-Sum Product Theorem

We will prove that, for any finite set A of reals,

$$\max\{|A+A|, |A \cdot A|\} = \Omega\Big(\frac{n^{1+(3/11)}}{(\log n)^{3/11}}\Big).$$

We will need the following lemma, often called the *Power Mean Inequality*. The proof is in the appendix.

Lemma 6.1 *For all nonnegative reals $n_1, \ldots, n_k$, and for all reals r,*

$$\sum_{i=1}^{k} \frac{n_i^r}{k} \geq \frac{(\sum_{i=1}^{k} n_i)^r}{k^{r-1}}.$$

We will prove the main theorem as a sequence of lemmas revolving around the following set.

Notation 6.2 For the rest of this section A is a fixed finite set of reals and

$$X = \{(a_1, a_2, a_3, a_4) : a_1, a_2, a_3, a_4 \in A \wedge \frac{a_1}{a_2} = \frac{a_3}{a_4}\}.$$

We will also use the equivalent formulation

$$X = \{(a_1, a_2, a_3, a_4) : a_1, a_2, a_3, a_4 \in A \wedge a_1 a_4 = a_2 a_3\}.$$

We will prove an upper bound, and a lower bound on $|X|$.
First a lower bound.

Lemma 6.3 $|X| \geq |A|^4/|A \cdot A|$.

Proof:

Let $A \cdot A = \{p_1, \ldots, p_k\}$. Note that $k = |A \cdot A|$. For all i, $1 \leq i \leq k$, let

$$N_i = \{(a, b) \in A \times A : ab = p_i\}.$$

$$n_i = |N_i|.$$

We first get an exact expression for $|X|$. Every element of $|X|$ is formed by first finding an element $p_i \in A \cdot A$ to be what $a_1 a_4 = a_2 a_3$ will be, and then finding the two ordered pairs in N_i to be the (a_1, a_4) and (a_2, a_3). Hence

$$|X| = \sum_{i=1}^{k} n_i^2.$$

The number of elements in $A \times A$ is clearly $|A|^2$. We now count the number of elements in $A \times A$ a different way. Every element of $A \times A$ can be though of as first picking the product p_i and then picking the elements that have that product. Hence

$$|A \times A| = \sum_{i=1}^{k} n_i.$$

But we also have $|A \times A| = |A|^2$. Hence

$$\sum_{i=1}^{k} n_i = |A|^2.$$

By Lemma 6.1, with $r = 2$, we have:

$$\left(\frac{\sum_{i=1}^{k} n_i}{k}\right)^2 \leq \frac{\sum_{i=1}^{k} n_i^2}{k}.$$

Since $\sum_{i=1}^{k} n_i = |A|^2$ and $\sum_{i=1}^{k} n_i^2 = |X|$ we have

$$\left(\frac{|A|^2}{k}\right)^2 \leq \frac{|X|}{k}$$

$$\frac{|A|^4}{k^2} \leq \frac{|X|}{k}$$

$$\frac{|A|^4}{k} \leq |X|$$

Recall that $k = |A \cdot A|$. Hence

$$|X| \geq \frac{|A|^4}{|A \cdot A|}.$$

∎

To get an upper bound on $|X|$ we need more concepts. We can assume $0 \notin A$. Now we do a thought experiment. Look at $A \times A$. Divide it up based on the *ratio* of the two numbers. That is, for every $m \in A/A$, we have a box

$$BOX_m = \{(x, y) : x, y \in A \wedge x/y = m\}.$$

Hence we have that $A \times A = \cup_{m \in A/A} BOX_m$. We order these boxes *not* by the numerical values of m— we do not care about that— but by how big the boxes are. Let $m_1, m_2, \ldots, m_{|A/A|}$ be such that

$$|BOX_{m_1}| \leq |BOX_{m_2}| \leq \cdots \leq |BOX_{m_{|A/A|}}|.$$

We could then group the boxes together as follows:
Let

$$BOX_{m_1}, \ldots, BOX_{m_{i_1}}$$

be all the boxes with cardinality in $[1, 2)$. Let

$$BOX_{m_{i_1+1}}, \ldots, BOX_{m_{i_2}}$$

be all the boxes with cardinality in $[2, 4)$. Let

$$BOX_{m_{i_2+1}}, \ldots, BOX_{m_{i_3}}$$

be all the boxes with cardinality in $[4, 8)$. And so on, via powers of two. With this in mind, here is a formal definition.

Def 6.4 Let

$$D_d = \{m \in A/A : d \leq |BOX_m| < 2d\}.$$

Notation 6.5

$$X_d = \{(a_1, a_2, a_3, a_4) : \frac{a_1}{a_2} = \frac{a_3}{a_4} \in D_d\}.$$

Notation 6.6 $POW2$ is the set of powers of 2.

Lemma 6.7

1. *If $d \geq |A| + 1$ then $D_d = \emptyset$.*
2. *For all d, $|X_d| \leq O(d^2|D_d|)$.*
3. *$|X| = \sum_{d \in POW2, d \leq |A|} |X_d|$.*

Proof:

1) We show that, for all m, $|BOX_m| \leq |A|$. Every element in BOX_m is an ordered pair $(a, a') \in A \times A$ such that $a/a' = m$. Map each element to its first component. This is a 1-1 mapping of BOX_m into $|A|$. Hence $|BOX_m| \leq |A|$.

Since $|BOX_m| \leq |A|$, we have that, for $d \geq |A| + 1$, $D_d = \emptyset$.

2) To form an element of $|X_d|$ you first pick an element $m \in D_d$ for the quotients to equal. You can do that in $|D_d|$ ways. You then pick two ordered pairs (a_1, a_2) and (a_3, a_4) such that $a_1/a_2 = a_3/a_4 = m$. How many ordered pairs can there be? By the definition of D_d there are between d and $2d$. Hence there are $O(d^2)$ ways to pick the ordered pairs. So we have

$$|X_d| = O(d^2|D_d|).$$

3) Let $POW2$ be the set of powers of 2. It is easy to see that

$$X = \bigcup_{d \in POW2} X_d.$$

By part (1) all $d \geq |A| + 1$ have $D_d = \emptyset$ and hence $X_d = \emptyset$. Therefore the union need only consider $d \leq |A|$. ∎

To get an upper bound on $|X|$ we will get an upper bound on $|X_d|$. To get an upper bound on $|X_d|$ we will get an upper bound on $|D_d|$.

Lemma 6.8

1. *Let $SLOPES$ and A be finite sets of reals such that $|SLOPES| \leq |A|^2$. Let*

$$L = \{\ell : \ell \text{ has slope in } SLOPES \text{ and has a point in } A \times A\}.$$

Then $|L| = \Omega(|A||SLOPES|^{3/2})$.

2. *Let $d \in \mathsf{N}$. Let*

$$L = \{\ell : \ell \text{ has slope in } D_d \text{ and has a point in } A \times A\}.$$

Then $|L| = \Omega(|A||D_d|^{3/2})$.

Proof:

1) We will be applying Lemma 4.1 and 4.2. Hence we will be defining sets of points and lines.

Look at the set

$$MEET = \{p : p \text{ is on } \geq |SLOPES| \text{ of the lines in } L\ \}.$$

We obtain upper and lower bounds on $|MEET|$.

Let $(x, y) \in A \times A$. For every $m \in SLOPES$ there is a line in L that goes through (x, y). Hence $(x, y) \in MEET$. Therefore

$$|MEET| \geq |A \times A| = |A|^2.$$

We apply Lemma 4.2 to L with $k = |SLOPES|$ to obtain

$$|MEET| \leq O\Big(\max\Big\{\frac{||L||^2}{|SLOPES|^3}, \frac{||L||}{|SLOPES|}\Big\}\Big).$$

There are two cases.

Case 1: $\frac{|L|}{|SLOPES|} \leq \frac{|L|^2}{|SLOPES|^3}$.

$$|A|^2 \leq |MEET| \leq O\Big(\frac{|L|^2}{|SLOPES|^3}\Big)$$

$$|L| = \Omega(|A||SLOPES|^{3/2}).$$

Case 2: $\frac{|L|^2}{|SLOPES|^3} \leq \frac{|L|}{|SLOPES|}$.

$$|A|^2 \leq |MEET| \leq O\Big(\frac{|L|}{|SLOPES|}\Big)$$

$$|L| = \Omega(|A|^2|SLOPES|) = \Omega(|A||A||SLOPES|).$$

Since $|SLOPES| \leq |A|^2$, $|A| \geq |SLOPES|^{1/2}$. Hence we get

$$|L| = \Omega(|A||A||SLOPES|) \geq \Omega(|A||SLOPES|^{1/2}|SLOPES|) = \Omega(|A||SLOPES|^{3/2}).$$

2) This follows from part (1) and the observation that since $D_j \subseteq A/A$, $|D_j| \leq |A|^2$.
∎

Lemma 6.9 *Let $d \in \mathsf{N}$. Then*

$$|D_d| \leq O\Big(\frac{|A + A|^{8/3}}{d^2|A|^{2/3}}\Big).$$

Proof:

Let

$$P = (A + A) \times (A + A).$$

Let

$$L = \{\ell : \ell \text{ has slope in } D_d \text{ and a point in } A \times A\}.$$

$$L' = \{\ell : \ell \text{ has} \geq d \text{ elements of } P \text{ on it } \}.$$

We show $L \subseteq L'$. Let $\ell \in L$. There exists $a_1, a_2, a_3, a_4 \in A$ such that ℓ has slope a_3/a_4 and passes through (a_1, a_2). Hence ℓ is described by the equation

$$y = \frac{a_3}{a_4}x + a_2 - \frac{a_1 a_3}{a_4}.$$

Let m be the slope, $m = \frac{a_3}{a_4}$. Note that by the definition of D_d there are at least d ordered pairs $(b_1, c_1), \ldots, (b_d, c_d) \in A \times A$ such that $b_i/c_i = m$. Hence, for all i, $1 \leq i \leq d$,

$$y = \frac{b_i}{c_i}x + a_2 - \frac{a_1 b_i}{c_i}.$$

Plug $x = a_1 + c_i$ into this. You get

$$y = \frac{b_i}{c_i}(a_1 + c_i) + a_2 - \frac{a_1 b_i}{c_i}$$

$$y = \frac{b_i a_1}{c_i} + b_i + a_2 - \frac{a_1 b_i}{c_i}$$

$$y = a_2 + b_i.$$

Hence the point $(a_1 + c_i, a_2 + b_i) \in P$ is on the line. This holds for any i, so every point in L has at least d elements of P on it. Therefore $L \subseteq L'$ and

$$|L| \leq |L'|$$

By Lemma 4.1 with $k = d$ we obtain

$$|L'| \leq \max\left\{\frac{|P|^2}{d^3}, \frac{|P|}{d}\right\}.$$

There are two cases.

Case 1: $\frac{|P|}{d} \leq \frac{|P|^2}{d^3}$.

$$|L| \leq |L'| \leq \frac{|P|^2}{d^3}.$$

Since $P = (A + A) \times (A + A)$, $|P| = |A + A|^2$. Hence

$$|L| \leq \frac{|A + A|^4}{d^3}.$$

By Lemma 6.8 we have

$$|L| = \Omega(|A||D_d|^{3/2}).$$

Hence we have

$$|A||D_d|^{3/2} \leq O(|L|) \leq \Big(\frac{|A+A|^4}{d^3}\Big).$$

$$|D_d|^{3/2} \leq O\Big(\frac{|A+A|^4}{d^3|A|}\Big).$$

$$|D_d| \leq O\Big(\frac{|A+A|^{8/3}}{d^2|A|^{2/3}}\Big).$$

Case 2: $\frac{|P|^2}{d^3} \leq \frac{|P|}{d}$.

$$|L| \leq |L'| \leq \frac{|P|}{d}.$$

Since $P = (A+A) \times (A+A)$, $|P| = |A+A|^2$. Hence

$$|L| \leq |L'| \leq \frac{|A+A|^2}{d}.$$

By Lemma 6.8 we have

$$|L| = \Omega(|A||D_d|^{3/2}).$$

Hence we have

$$|A||D_d|^{3/2} \leq O(|L|) \leq O\Big(\frac{|A+A|^2}{d}\Big).$$

$$|D_d|^{3/2} \leq O\Big(\frac{|A+A|^2}{d|A|}\Big).$$

$$|D_d| \leq O\Big(\frac{|A+A|^{4/3}}{d^{2/3}|A|^{2/3}}\Big) \leq O\Big(\frac{|A+A|^{4/3}d^{4/3}}{d^2|A|^{2/3}}\Big).$$

By Lemma 6.7.1 we know that, for $d \geq |A|+1$, $D_d = 0$. Hence we can assume $d \leq |A| \leq |A+A|$. With this we have

$$|D_d| \leq O\Big(\frac{|A+A|^{4/3}d^{4/3}}{d^2|A|^{2/3}}\Big) \leq O\Big(\frac{|A+A|^{4/3}|A+A|^{4/3}}{d^2|A|^{2/3}}\Big) \leq O\Big(\frac{|A+A|^{8/3}|}{d^2|A|^{2/3}}\Big)$$

∎

Lemma 6.10

$$|X| = O\Big(\frac{|A+A|^{8/3}(\log|A|)}{|A|^{2/3}}\Big).$$

Proof:

By Lemma 6.7.a

$$|X_d| = O(d^2|D_d|).$$

By Lemma 6.9

$$|D_d| \leq O\Big(\frac{|A+A|^{8/3}}{d^2|A|^{2/3}}\Big).$$

Hence

$$|X_d| \leq O\Big(\frac{|A+A|^{8/3}}{|A|^{2/3}}\Big).$$

Note that this bound is independent of d.

By Lemma 6.7.b and the above equation we have the following, where d ranges over the powers of 2 that are $\leq O(|A|)$.

$$|X| = \sum_d |X_d| = \sum_d O\Big(\frac{|A+A|^{8/3}}{|A|^{2/3}}\Big) = O\Big(\frac{|A+A|^{8/3}(\log|A|)}{|A|^{2/3}}\Big)$$

∎

Theorem 6.11 *Let A be a finite set of reals.*

1.

$$\max\{|A\cdot A|, |A+A|\} = \Omega\Big(\frac{|A|^{14/11}}{(\log|A|)^{3/11}}\Big).$$

2.

$$\max\{|A\cdot A|, |A/A|\} = \Omega(|A|^{14/11}).$$

Proof:

1) By Lemma 6.3 and 6.10

$$\frac{|A|^4}{|A\cdot A|} \leq |X| \leq O\Big(\frac{|A+A|^{8/3}(\log|A|)}{|A|^{2/3}}\Big).$$

$$\frac{|A|^{14/3}}{|A\cdot A|} \leq O(|A+A|^{8/3}(\log|A|)).$$

$$\frac{|A|^{14/3}}{\log|A|} \leq O(|A\cdot A||A+A|^{8/3})).$$

$$\frac{|A|^{14}}{(\log|A|)^3} \leq O(|A\cdot A|^3|A+A|^8).$$

Assume, by way of contradiction, that

$$|A \cdot A| << |A|^{14/11}/(\log|A|)^{3/11}$$

and

$$|A + A| << |A|^{14/11}/(\log|A|)^{3/11}.$$

Then

$$\frac{|A|^{14}}{(\log|A|)^3} \leq O(|A \cdot A|^3|A + A|^8) << O((|A|^{(14\cdot 3)/11}|A|^{(14\cdot 8)/11})/(\log|A|)^3.$$

$$|A|^{14} << O(|A|^{(14\cdot 3)/11}|A|^{(14\cdot 8)/11})$$

$$|A|^{14} << O(|A|^{14})$$

This is a contradiction.

2) By Lemma 6.9

$$|D_d| \leq O\Big(\frac{|A + A|^{8/3}}{d^2|A|^{2/3}}\Big).$$

Let

$$Y_d = \{(a_1, a_2) \in A \times A : \frac{a_1}{a_2} \in D_d\}.$$

By the definition of D_d

$$|Y_d| = O(dD_d) = O\Big(\frac{|A + A|^{8/3}}{d|A|^{2/3}}\Big)$$

and

$$\bigcup_{d \in POW2, d \leq |A|} Y_d = A \times A.$$

Hence

$$\sum_{d \in POW2, d \leq |A|} |Y_d| = |A|^2.$$

Let c be a parameter to be chosen later. We will split this sum up depending on if $d < \frac{c|A+A|^{8/3}}{|A|^{8/3}}$ or $d > \frac{c|A+A|^{8/3}}{|A|^{8/3}}$.

$$|A|^2 = \sum_{d \in POW2, d \leq \frac{c|A+A|^{8/3}}{|A|^{8/3}}} |Y_d| + \sum_{d \in POW2, d > \frac{c|A+A|^{8/3}}{|A|^{8/3}}} |Y_d|.$$

$$\leq \sum_{d\in POW2, d\leq \frac{c|A+A|^{8/3}}{|A|^{8/3}}} \frac{|A+A|^{8/3}}{d|A|^{2/3}} + \sum_{d\in POW2, d> \frac{c|A+A|^{8/3}}{|A|^{8/3}}} \frac{|A+A|^{8/3}}{d|A|^{2/3}}.$$

Consider the second summation.

$$\sum_{d\in POW2, d> \frac{c|A+A|^{8/3}}{|A|^{8/3}}} \frac{|A+A|^{8/3}}{d|A|^{2/3}} \leq O(c|A|^2).$$

Take c such that this quantity is $\leq \frac{|A|^2}{2}$.
We now have

$$\sum_{d\in POW2, d\leq \frac{c|A+A|^{8/3}}{|A|^{8/3}}} \frac{|A+A|^{8/3}}{d|A|^{2/3}} \geq \Omega(|A|^2).$$

Consider

$$Y = \bigcup_{d< \frac{c|A+A|^{8/3}}{|A|^{8/3}}} Y_d.$$

We map Y to A/A by mapping (a_1, a_2) to a_1/a_2. By the definition of Y_d and $d < \frac{c|A+A|^{8/3}}{|A|^{8/3}}$ this map is at most $\frac{c|A+A|^{8/3}}{|A|^{8/3}}$-to-1. Hence

$$|A/A| \geq \frac{|Y|}{\frac{c|A+A|^{8/3}}{|A|^{8/3}}} \geq \Omega\Big(\frac{|A|^2||A|^{8/3}}{|A+A|^{8/3}}\Big).$$

$$|A/A||A+A|^{8/3} \geq |A|^{14/3}.$$

$$|A/A|^3|A+A|^8 \geq |A|^{14}.$$

By reasoning similar to that at the end of part 1 of this theorem, we obtain the result.

∎

7 Appendix: The Power-Mean Inequality

Lemma 7.1 *For all nonnegative reals $n_1, \ldots, n_k$, and for all reals r,*

$$\sum_{i=1}^{k} \frac{n_i^r}{k} \geq \frac{(\sum_{i=1}^{k} n_i)^r}{k^{r-1}}.$$

Proof: Consider the following problem: Given M, minimize $\sum_{i=1}^k x_i^r$ subject to the constraints $\sum_{i=1}^k x_i = M$. First look at the $k = 2$ case.

We want to minimize $x^r + y^r$ subject to the constraint that $x+y = M$ and $x, y \geq 0$. Hence we want to minimize

$x^r + (M-x)^r$ subject to $x \in [0, M]$.

Using calculus one easily finds that this is minimized when $x = M - x$ or when $x = y = M/2$.

The min for the general problems occurs when all x_i are M/k. This is because, by the $k = 2$ case, if you have a solution where there is an i, j such that $x_i < x_j$ you can make it smaller by replacing both with $(x_i + x_j)/2$. Hence

$$\min\{\sum_{i=1}^k x_i^r \mid \sum_{i=1}^k x_i = M\} = \sum_{i=1}^k \Big(\frac{M}{k}\Big)^r = \frac{M^r}{k^{r-1}}.$$

Let $n_1, \ldots, n_k$ be positive reals. Let $M = \sum_{i=1}^k n_k$.

$$\sum_{i=1}^k \frac{n_i^r}{k} \geq \min\{\sum_{i=1}^k x_i^r \mid \sum_{i=1}^k x_i = M\} = \frac{M^r}{k^{r-1}} = \frac{(\sum_{i=1}^k n_i)^r}{k^{r-1}}.$$

∎

References

[1] M. Ajtai, V. Chvátal, M. Newborn, and E. Szemerédi. Crossing free subgraphs. *Annals of Discrete Mathematics*, 12:9–12, 1982.

[2] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geometric and Functional Analysis*, 14:27–57, 2004. `http://arxiv.org/abs/math.NT/0304217`.

[3] M. Chang. Additive and multiplicative structure in matrix space. This paper is referenced in The Tao-Vu book *Additive Combinatorics* but I have not been able to find it anywhere.

[4] Y.-G. Chen. On the sums and products of integers. *Proceedings of the American Math Society*, 127:1927–1933, 1999. `http://www.jstor.org/`.

[5] G. Elekis. On the number of sums and products. *Acta Arithmetica*, 81:365–367, 1997.

[6] K. Ford. Sums and products from a finite set of real numbers. *Ramanjuan Journal*, 2:59–66, 1998. `http://www.math.uiuc.edu/~ford/papers.html`.

[7] F. T. Leighton. *Complexity issues in VLSI.* MIT Press, 1983.

[8] M. B. Nathanson. On the sums and products of integers. *Proceedings of the American Math Society*, 125:9–15, 1997. http://www.jstor.org/.

[9] J. Pach and P. Agarwal. *Combinatorial Geometry*. Wiley, 1995.

[10] J. Pach, R. Radoicic, G. Tardos, and T. Toth. Improving the Crossing Lemma by finding more crossings in sparse graphs. *Discrete & Computational Geometry*, pages 527–552, 2006. Earlier version in 20th Annual Symposium on Comp. Geom. Current version at http://www.renyi.hu/~tardos/.

[11] J. Solymosi. On the number of sums and products. *Bulletin of the London Mathematical Society*, 37:491–494, 2005. http://blms.oxfordjournals.org/content/by/year.

[12] L. Székely. Crossing numbers and hard Erdős problems in discrete geometry. *Combinatorics, Probability and Computing*, 11:1–10, 1993. http://www.cs.umd.edu/~gasarch/TOPICS/erdos_dist/erdos_dist.html.

[13] E. Szemerédi and W. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3:381–392, 1983. http://www.springer.com/new+%26+forthcoming+titles+%28default%29/journal/493.

[14] P. E. E. Szemerédi. On the sums and products of integers. In Erdős, Alpar, Halasz, and Sárközy, editors, *Studies in Pure Mathematics*, pages 213–218, 1983. http://www.renyi.hu/~p_erdos/Erdos.html.

[15] T. Tao and V. Hu. *Additive Combinatorics*. Cambridge University Press, 2006.

[16] A. Wigderson. The Sum-Product theorem and applications, 2006. http://www.math.ias.edu/~avi/TALKS/ This is a talk, not a paper.