8 Sum-Product Problem

Chapter Highlights

- The sum-product problem: showing that one of $A + A$ and $A \cdot A$ must be large
- Crossing number inequality: lower bound on the number of crossings in a graph drawing
- Szemerédi–Trotter theorem on point-line incidences
- Eleke's sum-product bound using incidence geometry
- Solymosi's sum-product bound via multiplicative energy

In the previous chapter we studied the **sumset**

$$A + A := \{a + b : a, b \in A\} .$$

Likewise we can also consider the **product set**

$$A \cdot A = AA := \{ab : a, b \in A\}$$

Question 8.0.1 (Sum-product problem)
Can the sumset and the product set be simultaneously small?

Arithmetic progressions have small additive doubling, while geometric progressions have small multiplicative doubling. However, perhaps a set cannot simultaneously look both like an arithmetic and a geometric progression.

Erdős and Szemerédi (1983) conjectured that at least one of $A + A$ and AA is close to quadratic size.

Conjecture 8.0.2 (Sum-product conjecture)
For every finite subset A of $\mathbb{R}$, we have

$$\max \{|A + A|, |AA|\} \geq |A|^{2-o(1)} .$$

Here $o(1)$ is some quantity that goes to zero as $|A| \to \infty$.

Erdős and Szemerédi (1983) proved bounds of the form

$$\max \{|A + A|, |AA|\} \geq |A|^{1+c}$$

for some constant $c > 0$. In this chapter, we will give two different proofs of the above form. First, we present a proof by Elekes (1997) using incidence geometry, in particular a seminal theorem of Szemerédi and Trotter (1983) on the incidences of points and lines. Second, we present a proof by Solymosi (2009) using multiplicative energy, which gives nearly the best bound to date.

8.1 Multiplication Table Problem

Let us first explain why we need the error term $-o(1)$ in the exponent in Conjecture 8.0.2. Erdős (1955) posed the following problem.

Question 8.1.1 (Erdős multiplication table problem)
What is the size of $[N] \cdot [N]$, i.e., the number of distinct entries that appear in the multiplication table?

1	2	3	4	5	6	7	8	9	10	$\cdots$
2	4	6	8	10	12	14	16	18	20	$\cdots$
3	6	9	12	15	18	21	24	27	30	$\cdots$
4	8	12	16	20	24	28	32	36	40	$\cdots$
5	10	15	20	25	30	35	40	45	50	$\cdots$
6	12	18	24	30	36	42	48	54	60	$\cdots$
7	14	21	28	35	42	49	56	63	70	$\cdots$
8	16	24	32	40	48	56	64	72	80	$\cdots$
9	18	27	36	45	54	63	72	81	90	$\cdots$
10	20	30	40	50	60	70	80	90	100	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

After much work, we now have a satisfactory answer. A precise estimate was given by Ford (2008):

$$|[N] \cdot [N]| = \Theta\left(\frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}\right)$$

where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$. Here we give a short proof of some weaker estimates (Erdős 1955).

Theorem 8.1.2 (Estimates on the multiplication table problem)

$$(1 - o(1))\,\frac{N^2}{2\log N} \le |[N] \cdot [N]| = o(N^2)$$

This already show that is false that at least one of $A + A$ and AA has size $\geq c\,|A|^2$. So we cannot remove the $-o(1)$ term from the exponent in the sum-product conjecture.

To prove Theorem 8.1.2, we apply the following fact from number theory due to Hardy and Ramanujan (2000). A short probabilistic method proof was given by Turán (1934); also see Alon and Spencer (2016, Section 4.2).

Theorem 8.1.3 (Hardy–Ramanujan)
All but $o(N)$ positive integers up to N have $(1+o(1))\log\log N$ prime factors counted with multiplicity.

Proof of Theorem 8.1.2. First let us prove the upper bound. By the Hardy–Ramanujan theorem, all but at most $o(N^2)$ of the elements of $[N]\cdot[N]$ have $(2+o(1))\log\log N$ prime factors. However, by the Hardy–Ramanujan theorem again, all but $o(N^2)$ of positive integers $\leq N^2$ have $(1+o(1))\log\log(N^2) = (1+o(1))\log\log N$ prime factors, and thus cannot appear in $[N]\cdot[N]$. Hence $|[N]\cdot[N]| = o(N^2)$. (Remark: this proof gives $|[N]\cdot[N]| = O(N^2/\log\log N)$.)

Now let us prove the lower bound by giving a lower bound to the number of positive integers $\leq N^2$ of the form pm, where p is a prime in $(N^{2/3}, N]$ and $m \leq N$. Every such n has at most 2 such representations as pm since $n \leq N^2$ can have at most two prime factors greater than $N^{2/3}$. There are $(1+o(1))N/\log N$ primes in $(N^{2/3}, N]$ by the prime number theorem. So the number of distinct such pm is $\geq (1/2 - o(1))N^2/\log N$. □

Remark 8.1.4. The lower bound (up to a constant factor) also follows from Solymosi's sum-product estimate that we will see later in Theorem 8.3.1.

8.2 Crossing Number Inequality and Point-Line Incidences

The goal of this section is to give a proof of the following sum-product estimate, due to Elekes (1997), using incidence geometry. Recall we use $f \gtrsim g$ to mean that $f \geq cg$ for some constant $c > 0$.

Theorem 8.2.1 (Elekes' sum-product bound)
Every finite $A \subset \mathbb{R}$ satisfies

$$|A + A|\,|AA| \gtrsim |A|^{5/2}.$$

Corollary 8.2.2 (Elekes' sum-product bound)
Every finite $A \subset \mathbb{R}$ satifies

$$\max\{|A + A|, |AA|\} \gtrsim |A|^{5/4}.$$

We introduce a basic result from geometric graph theory.

Crossing number inequality

The **crossing number** $\mathrm{cr}(G)$ of a graph G is defined to be the minimum number of edge crossings in a planar drawing of G where edges are drawn with continuous curves.

The next theorem shows that every drawing of a graph with many edges necessarily has lots of edge crossings. For example, it implies that every n-vertex graph with $\Omega(n^2)$ edges has $\Omega(n^4)$ crossings, i.e., a constant fraction of the edges must cross in a dense graph. This result is independently due to Ajtai, Chvátal, Newborn, and Szemerédi (1982) and Leighton (1984).

Theorem 8.2.3 (Crossing number inequality)
Every graph $G = (V, E)$ with $|E| \geq 4\,|V|$ has

$$\mathrm{cr}(G) \gtrsim \frac{|E|^3}{|V|^2}.$$

Proof. For any connected planar graph $G = (V, E)$ with at least one cycle, we have $3\,|F| \leq 2\,|E|$, with $|F|$ denoting the number of faces (including the outer face). The inequality follows from double counting using that every face is adjacent to at least three edges and that every edge is adjacent to at most two faces. By Euler's formula, $|V| - |E| + |F| = 2$. Replacing $|F|$ using $3\,|F| \leq 2\,|E|$, we obtain $|E| \leq 3\,|V| - 6$. Therefore $|E| \leq 3\,|V|$ holds for every planar graph G including ones that are not connected or do not have a cycle.

If an arbitrary graph $G = (V, E)$ satisfies $|E| > 3\,|V|$, then any drawing of G can be made planar by deleting at most $\mathrm{cr}(G)$ edges, one for each crossing. It follows that $|E| - \mathrm{cr}(G) \geq 3\,|V|$. Therefore, the following inequality holds universally for all graphs $G = (V, E)$:

$$\mathrm{cr}(G) \geq |E| - 3\,|V|. \tag{8.2.1}$$

Now we apply a probabilistic method technique to "boost" the above inequality to denser graphs. Let $G = (V, E)$ be a graph with $|E| \geq 4\,|V|$. Let $p \in [0, 1]$ be some real number to be determined and let $G' = (V', E')$ be a graph obtained by independently randomly keeping each vertex of G with probability p. By (8.2.1), we have $\mathrm{cr}(G') \geq |E'| - 3\,|V'|$ for every G'. Therefore the same inequality must hold if we take the expected values of both sides:

$$\mathbb{E}\,\mathrm{cr}(G') \geq \mathbb{E}\,|E'| - 3\mathbb{E}\,|V'|.$$

We have $\mathbb{E}\,|E'| = p^2\,|E|$ since an edge remains in G' if and only if both of its endpoints are kept. Similarly $\mathbb{E}\,|V'| = p\,|V|$. By keeping the same drawing, we get the inequality $p^4\,\mathrm{cr}(G) \geq \mathbb{E}\,\mathrm{cr}(G')$. Therefore

$$\mathrm{cr}(G) \geq p^{-2}\,|E| - 3p^{-3}\,|V|.$$

Finally set $p = 4|V|/|E| \in [0,1]$ (here we use $|E| \geq 4|V|$) to get $\mathrm{cr}(G) \gtrsim |E|^3/|V|^2$. □

Szemerédi–Trotter theorem on point-line incidences

Given a set of points $\mathcal{P}$ and the set of lines $\mathcal{L}$, define the number of incidences to be

$$I(\mathcal{P}, \mathcal{L}) := |\{(p, \ell) \in \mathcal{P} \times \mathcal{L} : p \in \ell\}|$$

Question 8.2.4 (Point-line incidence)
What's the maximum number of incidences between n points and m lines?

One trivial upper bound is $|\mathcal{P}|\,|\mathcal{L}|$. We can get a better bound by using the fact that every pair of points is determined by at most one line:

$$\begin{aligned} |\mathcal{P}|^2 &\geq |\{(p, p', \ell) \in \mathcal{P} \times \mathcal{P} \times \mathcal{L} : pp' \in \ell,\ p \neq p'\}| \\ &\geq \sum_{\ell \in \mathcal{L}} |\mathcal{P} \cap \ell|(|\mathcal{P} \cap \ell| - 1) \geq \frac{I(\mathcal{P}, \mathcal{L})^2}{|\mathcal{L}|^2} - I(\mathcal{P}, \mathcal{L}). \end{aligned}$$

The last inequality follows from Cauchy–Schwarz inequality. Therefore,

$$I(\mathcal{P}, \mathcal{L}) \leq |\mathcal{P}|\,|\mathcal{L}|^{1/2} + |\mathcal{L}|\,.$$

By the same argument with the roles of points and lines swapped (or by applying point-line duality),

$$I(\mathcal{P}, \mathcal{L}) \leq |\mathcal{L}|\,|\mathcal{P}|^{1/2} + |\mathcal{P}|\,.$$

In particular these inequalities tell us that n points and n lines have $O(n^{3/2})$ incidences.

The above bound only uses the fact that every pair of points determines at most one line. Equivalently, we are only using that the bipartite point-line incidence graph is 4-cycle-free. So the $O(n^{3/2})$ bound (and the above proof) is the same as the $K_{2,2}$-free extremal number bound from Section 1.4. Also, the $O(n^{3/2})$ bound is tight for the finite field projective plane over $\mathbb{F}_q$ with $n = q^2 + q + 1$ points and $n = q^2 + q + 1$ lines gives $n(q+1) \sim n^{3/2}$ incidences (this the same construction showing that $\mathrm{ex}(n, K_{2,2}) \gtrsim n^{3/2}$ in Theorem 1.10.1).

On the other hand, in the real plane, the $n^{3/2}$ bound can be substantially improved. The following seminal result due to Szemerédi and Trotter (1983) gives a tight estimate on the number of point-line incidences in the real plane.

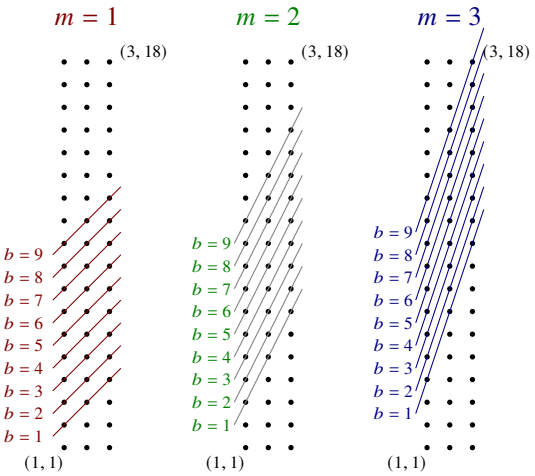
Theorem 8.2.5 (Szemerédi–Trotter theorem)
For any set $\mathcal{P}$ of points and $\mathcal{L}$ of lines in $\mathbb{R}^2$,

$$I(\mathcal{P}, \mathcal{L}) \lesssim |\mathcal{P}|^{2/3}\,|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|$$

Corollary 8.2.6
The number of point-line incidences between n points and n lines in $\mathbb{R}^2$ is $O(n^{4/3})$.

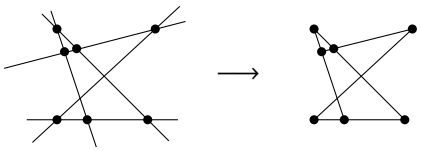
We will see a short proof using the crossing number inequality due to Székely (1997). Since the inequality is false over finite fields, any proof necessarily requires the topology of the real plane (via the application of Euler's theorem in the proof of the crossing number inequality).

Example 8.2.7. The bounds in both Theorem 8.2.5 and Corollary 8.2.6 are best possible up to a constant factor. Here is an example showing that Corollary 8.2.6 is tight. Let $\mathcal{P} = [k] \times [2k^2]$ and $\mathcal{L} = \{y = mx + b : m \in [k], b \in [k^2]\}$. Then every line in $\mathcal{L}$ contains k points from $\mathcal{P}$, so $I(\mathcal{P}, \mathcal{L}) = k^4 = \Theta(n^{4/3})$.



Proof of Theorem 8.2.5. We remove all lines in $\mathcal{L}$ containing at most one point in $\mathcal{P}$. These lines contribute to at most $|\mathcal{L}|$ incidences and thus does not affect the inequality we wish to prove.

Now assume that every line in $\mathcal{L}$ contains at least two points of $\mathcal{P}$. Turn every point of $\mathcal{P}$ into a vertex and each line in $\mathcal{L}$ into edges connecting consecutive points of $\mathcal{P}$ on the line. This constructs a drawing of a graph $G = (V, E)$ on the plane.



Assume that $I(\mathcal{L}, \mathcal{P}) \geq 8|\mathcal{P}|$ holds (otherwise we are done as $I(\mathcal{P}, \mathcal{L}) \lesssim |\mathcal{P}|$). Each line in $\mathcal{L}$ with k incidences has $k - 1 \geq k/2$ edges. So $|E| \geq I(\mathcal{P}, \mathcal{L})/2 \geq 4|V|$. The crossing number inequality (Theorem 8.2.3) gives

$$\operatorname{cr}(G) \gtrsim \frac{|E|^3}{|V|^2} \gtrsim \frac{I(\mathcal{P}, \mathcal{L})^3}{|\mathcal{P}|^2}.$$

Moreover $\operatorname{cr}(G) \leq |\mathcal{L}|^2$ since every pair of lines intersect in at most one point. Rearranging gives $I(\mathcal{P}, \mathcal{L}) \lesssim |P|^{2/3}|L|^{2/3}$. (Remember the linear contributions $|\mathcal{P}| + |\mathcal{L}|$ that need to be added back in due to the assumptions made earlier in the proof.) □

Now we are ready to prove the sum-product estimate in Theorem 8.2.1 for $A \subset \mathbb{R}$:

$$|A + A||AA| \gtrsim |A|^{5/2}.$$

Proof of Theorem 8.2.1. In $\mathbb{R}^2$, consider a set of points

$$\mathcal{P} = \{(x, y) : x \in A + A, y \in AA\}$$

and a set of lines

$$\mathcal{L} = \{y = a(x - a') : a, a' \in A\}.$$

For a line $y = a(x - a')$ in $\mathcal{L}$, $(a' + b, ab) \in \mathcal{P}$ is on the line for all $b \in A$, so each line in $\mathcal{L}$ contains $\geq |A|$ incidences. By definition of $\mathcal{P}$ and $\mathcal{L}$, we have

$$|\mathcal{P}| = |A + A||AA| \qquad \text{and} \qquad |\mathcal{L}| = |A|^2.$$

By the Szemerédi–Trotter theorem (Theorem 8.2.5),

$$\begin{aligned} |A|^3 = |A||\mathcal{L}| \leq I(\mathcal{P}, \mathcal{L}) &\lesssim |\mathcal{P}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}| \\ &\lesssim |A + A|^{2/3}|AA|^{2/3}|A|^{4/3}. \end{aligned}$$

The contributions from $|\mathcal{P}| + |\mathcal{L}|$ are lower order as $|\mathcal{P}| = |A + A||AA| \leq |A|^4 = |\mathcal{L}|^2$ and $|\mathcal{L}| = |A|^2 \leq |A + A|^2|AA|^2 = |\mathcal{P}|^2$. Rearranging the above inequality gives

$$|A + A||AA| \gtrsim |A|^{5/2}.$$ □

In Section 1.4, we proved an $O(n^{3/2})$ upper bound on the unit distance problem (Question 1.4.6) using the extremal number of $K_{2,3}$. The next exercise gives an improved bound (in fact the best known result to date).

Exercise 8.2.8 (Unit distance bound)**.** Using the crossing number inequality, prove given n points in the plane, at most $O(n^{4/3})$ pairs of points are separated by exactly unit distance.

8.3 Sum-Product via Multiplicative Energy

In this chapter, we give a different proof that gives a better sum-product estimate, due to Solymosi (2009).

Theorem 8.3.1 (Solymosi's sum-product bound)
Every finite set A of positive reals satisfies

$$|AA|\,|A+A|^2 \gtrsim \frac{|A|^4}{\log|A|}$$

Corollary 8.3.2 (Solymosi's sum-product bound)
Every finite $A \subset \mathbb{R}$ satisfies

$$\max\{|A+A|, |AA|\} \geq |A|^{4/3-o(1)}.$$

Proof of Theorem 8.3.1. We define **multiplicative energy** of A to be

$$E_\times(A) := |\{(a,b,c,d) \in A\times A\times A\times A : ab = cd\}|$$

Note that the multiplicative energy is a multiplicative version of additive energy. As with additive energy, having small multiplicative doubling implies large multiplicative energy, as seen by an application of the Cauchy–Schwarz inequality:

$$E_\times(A) = \sum_{x\in AA} \left|\{(a,b)\in A^2 : ab = x\}\right|^2 \geq \frac{|A|^4}{|AA|}.$$

Let

$$A/A := \{a/b : a,b \in A\}.$$

Write

$$r(s) = |\{(a,b)\in A\times A : s = a/b\}|.$$

We have

$$E_\times(A) = \sum_{s\in A/A} r(s)^2.$$

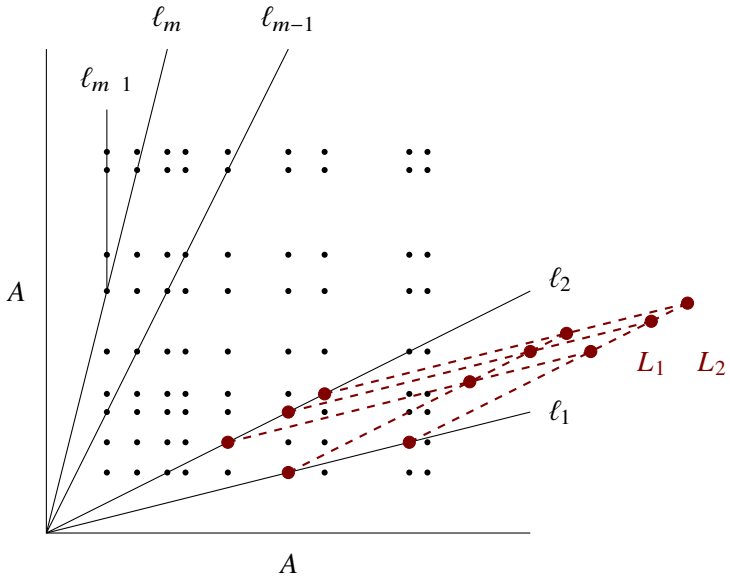
By pigeonhole principle (dyadic partitioning), there exists some nonnegative integer $k \lesssim \log|A|$ such that, setting

$$D = \{s : 2^k \leq r(s) \leq 2^{k+1}\} \quad \text{and} \quad m = |D|,$$

one has

$$\frac{E_\times(A)}{\log|A|} \lesssim \sum_{s\in D} r(s)^2 \leq m2^{2k+2}. \tag{8.3.1}$$

Let the elements of D be $s_1 < s_2 < \cdots < s_m$. For each $i \in [m]$, let ℓ_i be the line $y = s_i x$. Let ℓ_{m+1} be the vertical ray $x = \min(A)$ above ℓ_m.



Let $L_j = (A \times A) \cap \ell_j$. Then, for each $1 \le j \le m$,

$$|L_j| = r(s_j) \ge 2^k.$$

Furthermore, $|L_{m+1}| \ge |L_m| \ge 2^k$ as well.

Since ℓ_j and ℓ_{j+1} are not parallel, we have $|L_j + L_{j+1}| = |L_j||L_{j+1}|$. Moreover, the sets $L_j + L_{j+1}$ are disjoint for different j. The sumset $A \times A + A \times A$ (here $A \times A$ is the cartesian product) contains $L_j + L_{j+1}$ for each $1 \le j \le m$, so, using (8.3.1),

$$|A + A|^2 = |A \times A + A \times A| \ge \sum_{j=1}^{m} |L_j + L_{j+1}| = \sum_{j=1}^{m} |L_j||L_{j+1}| \ge m2^{2k} \gtrsim \frac{E_\times(A)}{\log |A|}.$$

Combining with $E_\times(A) \ge |A|^4 / |AA|$, which we obtained at the beginning of the proof, we obtain

$$|A + A|^2 \, |AA| \log |A| \gtrsim |A|^4 . \qquad \square$$

Remark 8.3.3 (Improvements). Konyagin and Shkredov (2015) improved Solymosi's sum-product bound to $\max\{|A + A|, |AA|\} \ge |A|^{4/3+c}$ for a small constant $c > 0$. This constant c was improved in subsequent works, but still remains quite small.

Remark 8.3.4 (Sum-product in $\mathbb{F}_p$)**.** Bourgain, Katz, and Tao (2004), combined with a later result of Bourgain, Glibichuk, and Konyagin (2006), proved the following sum-product estimate in $\mathbb{F}_p$ with p prime:

Theorem 8.3.5 (Sum-product in prime finite fields)
For every $\epsilon > 0$ there exists $\delta > 0$ and $c > 0$ so that every $A \subset \mathbb{F}_p$, with p prime, and $1 < |A| < p^{1-\epsilon}$, satisfies

$$\max\{|A+A|, |AA|\} \geq c\,|A|^{1+\delta}.$$

The statement is false over non-prime fields, since we could take A to be a subfield. Informally, the above theorem says that a prime field does not have any approximate sub-rings.

Chapter Summary

- **Sum-product conjecture.** $\max\{|A+A|, |AA|\} \geq |A|^{2-o(1)}$ for all $A \subset \mathbb{R}$.
- **Elekes' bound:** $\max\{|A+A|, |AA|\} \gtrsim |A|^{5/4}$
  - Proof uses point-line incidences.
  - **Crossing number inequality.** Every graph G with n vertices and $m \geq 4n$ edges has $\gtrsim m^3/n^2$ crossings in every drawing.
  - **Szemerédi–Trotter theorem.** m lines and n points in $\mathbb{R}^2$ form $O(m^{2/3}n^{2/3} + m + n)$ incidences.
- **Solymosi's bound:** $\max\{|A+A|, |AA|\} \gtrsim |A|^{4/3-o(1)}$.

Further Reading

Dvir's survey *Incidence Theorems and Their Applications* (2012) discusses many interesting related topics including incidence geometry and additive combinatorics together with their applications to computer science.

Guth's book *The Polynomial Method in Combinatorics* (2016) gives an in-depth discussion of incidence geometry in $\mathbb{R}^2$ and $\mathbb{R}^3$ leading to a proof of the solution of the Erdős distinct distances problem by Guth and Katz (2015).

Sheffer's book *Polynomial Methods and Incidence Theory* (2022) provides an introduction to incidence geometry and related topics.