A course on sum-product bounds

Frank de Zeeuw

May 29, 2017

This is a draft of the lecture notes for the second half of the course *Additive Combinatorics* at EPFL.

Chapter 1

Sum-product bounds in $\mathbb{R}$

1.1 Introduction

Given sets A, B in a field $\mathbb{F}$, we define the *sumset*

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

and the *productset*

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

We will study lower bounds for the sizes of these sets, and in particular the interaction between the sizes of sumsets and productsets. Individually, it is easy to give tight lower bounds, as the following proposition shows.

Proposition 1.1. *For $A \subset \mathbb{R}$ we have $|A + A| \geq 2|A| - 1$, with equality if and only if A is an arithmetic progression. Similarly, for $A \subset \mathbb{R}_{>0}$ we have $|A \cdot A| \geq 2|A| - 1$, with equality if and only if A is a geometric progression.*

Proof. Write the elements of A as $a_1 < \cdots < a_N$. The numbers

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_N < a_2 + a_N < \cdots < a_N + a_N$$

are clearly distinct, which implies $|A + A| \geq 2N - 1$. On the other hand, for any i the numbers

$$a_1+a_1 < a_1+a_2 < \cdots < a_1+a_i < a_2+a_i < \cdots < a_i+a_i < \cdots < a_i+a_N < \cdots < a_N+a_N$$

are also all distinct. If $|A + A| = 2|A| - 1$, these distinct sequences must be identical. In particular, looking at the $(i + 1)$-th entry, we see that $a_1 + a_{i+1} = a_2 + a_i$, so we have $a_{i+1} - a_i = a_2 - a_1$ for all i. This means that A is an arithmetic progression. Conversely, if $A = \{a + id : i = 1, \ldots, |A|\}$, then $|A + A| = |\{a + id : i = 2, \ldots, 2|A|\}| = 2|A| - 1$.

For $A \cdot A$, we can argue similarly with multiplication instead of addition, or we can apply the above to $\log(A) = \{\log(a) : a \in A\}$, together with $\log(A) + \log(A) = \log(A \cdot A)$, and the fact that if $\log(A)$ is an arithmetic progression, then A is a geometric progression. □

There are stronger versions of the observation that a set with a small sumset must resemble an arithmetic progression. The most significant such statement is Freiman's Theorem, which says that if $|A + A| \leq K|A|$, then A must be contained in a set of the form $\{a + i_1 d_1 + \cdots + i_k d_k : 1 \leq i_j \leq \ell\}$, with the parameters k, ℓ depending on K in a certain way. The proof is fairly difficult, and we do not include it in these notes.

If A is an arithmetic progression, then $|A+A|$ is small, but $|A\cdot A|$ is large; one can show with number-theoretic techniques that $|A\cdot A| \gg |A|^{2-\varepsilon}$ for any $\varepsilon > 0$. Conversely, if A is a geometric progression, then $|A+A|$ will be similarly large. This led Erdős and Szemerédi [5] to conjecture that for any set, either the sumset or the productset is large. Specifically, they proved that for any $A \subset \mathbb{Z}$ we have

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+\alpha}$$

for some $\alpha > 0$, and they conjectured that this holds for any $\alpha < 1$. This type of bound is what we call a *sum-product bound*. Others later observed that similar bounds hold for $A \subset \mathbb{R}$. In the next section, we will see the original proof of Erdős and Szemerédi, and then we will look at the various improvements that followed.

It is natural to consider the question of Erdős and Szemerédi over other fields than $\mathbb{R}$, like $\mathbb{C}$ or a finite field $\mathbb{F}_q$. One immediately encounters an obstacle if the field has non-trivial finite subfields (for instance, $\mathbb{F}_{p^2}$ has the subfield $\mathbb{F}_p$), since if A is a finite subfield of $\mathbb{F}$, then $A+A=A$ and $A\cdot A = A$ (in fact, even Proposition 1.1 would not hold). One can still obtain statements of the same flavor if one somehow excludes A from being a subfield, but proving such statements is more difficult. In a later chapter we will prove a sum-product bound over arbitrary fields, in which A is required to be small compared to the characteristic of the field. In the current chapter, we focus on the reals, where we can prove relatively good bounds using the ordering of the reals.

There are other instances of the "sum-product phenomenon" beside lower bounds for $\max\{|A+A|, |A\cdot A|\}$. For instance, one can prove a lower bound for the size of

$$A + A\cdot A = \{a + bc : a, b, c \in A\},$$

capturing the fact that, because $a+bc$ involves both addition and multiplication, neither an arithmetic nor a geometric progression can make $A + A\cdot A$ small. Let us give a proof of such a bound for integers, which appears to be the easiest example of a sum-product-type bound. The result has probably been known for longer, but we first heard this argument from Shakan [21].

Proposition 1.2. *For $A \subset \mathbb{N}$ we have*

$$|A + A\cdot A| \geq |A|^2 + |A| - 1,$$

and this inequality is tight.

Proof. Write $A = \{a_1 < \cdots < a_N\}$. The sets $a_i + a_N \cdot A$ are all disjoint, since each lies in a unique congruence class modulo a_N. We have $|A|$ such sets of size $|A|$, giving $|A|^2$ distinct elements of $A+A\cdot A$. Moreover, the $|A|-1$ numbers $a_1+a_1a_1, a_1+a_1a_2, \ldots, a_1+a_1a_{N-1}$ are smaller than all those counted so far, so we get at least $|A|^2+|A|-1$ numbers in total. On the other hand, it is not hard to see that for $A = \{1, \ldots, N\}$ we have $A+A\cdot A = \{2, \ldots, N^2+N\}$, which proves that the inequality is tight. □

Unfortunately, the proof does not seem to extend to fields, not even to $\mathbb{Q}$, but it has been conjectured that $|A+A\cdot A| \gg |A|^2$ for any $A \subset \mathbb{R}$. We will see that the arguments that lead to bounds for $\max\{|A+A|, |A\cdot A|\}$ often also lead to lower bounds for $|A + A\cdot A| \gg |A|^2$.

Similarly, other sum-product-type bounds can be proved for, for instance, the sets

$$A + A^2, \quad A + 1/A, \quad A(A+A), \quad AA + AA,$$

each of which has size larger than $|A|^{1+\beta}$ for some $\beta > 0$ (at least over $\mathbb{R}$).

1.2 The Erdős-Szemerédi Theorem

We now present a version of the original proof of the following sum-product bound of Erdős and Szemerédi [5].

Theorem 1.3 (Erdős–Szemerédi). *For $A \subset \mathbb{R}$ we have*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{32/31}.$$

We begin with the following observation. Note that the proof of this lemma would work in any field, but this is not the case for the proofs of the two lemmas that follow.

Lemma 1.4. *For any $B \subset \mathbb{R}$, there is a set $X_B \subset \mathbb{R}$ of size $|X_B| \leq |B|^4$ such that for any $C \subset \mathbb{R} \backslash X_B$ of size $|B|$ we have $\max\{|B+C|, |B \cdot C|\} \gg |B|^{4/3}$.*

Proof. Let $C \subset \mathbb{R}$ be any set of size $|B|$. Suppose that $|B+C|, |B \cdot C| < |B|^{4/3}$. Then $|B+C| < |B|^{4/3}$ implies that some element of $B+C$ is represented in $m \geq |B|^{2/3}$ ways, i.e., there are $b_1, \dots, b_m$ and $c_1, \dots, c_m$ such that $b_i + c_i = b_j + c_j$ for all i, j.

Consider the products $b_i \cdot c_j$ for all pairs i, j, of which there are at least $|B|^{4/3}$. Since we have $|B \cdot C| < |B|^{4/3}$, two of these products must coincide, i.e., we have a solution b_k, b_l, c_i, c_j with $k \neq l$ of $b_k \cdot c_i = b_l \cdot c_j$. Then $b_i, b_j, b_k, b_l, c_i, c_j$ form a solution of the pair of equations

$$b_i + c_i = b_j + c_j, \quad b_k \cdot c_i = b_l \cdot c_j.$$

In these two equations, b_i, b_j, b_k, b_l determine c_i, c_j uniquely; specifically we have $c_i = b_l(b_i - b_j)/(b_k - b_l)$ and $c_j = b_k(b_i - b_j)/(b_k - b_l)$.

We let X_B be the set of all such c_i, i.e.

$$X_B = \{b_4(b_1 - b_2)/(b_3 - b_4) : b_1, b_2, b_3, b_4 \in B\}.$$

We have $|X_B| \leq |B|^4$. For a set C disjoint from X_B, the argument above would lead to a contradiction. □

We cannot apply the lemma above directly to the set A, since X_A may turn out to contain A. However, we can apply it to a small subset $B \subset A$, say with $|B| = |A|^{1/5}$, so that X_B is only a small subset of A. Then for any $C \subset A \backslash X_B$ we have $\max\{|B+C|, |B \cdot C|\}$ relatively large (although much smaller than $|A|$). We will carefully choose B and many such C_i, in such a way that all $B + C_i$ are disjoint and all $B \cdot C_i$ are disjoint, so that we can sum up all these bounds $\max\{|B+C_i|, |B \cdot C_i|\}$ to get a bound larger than $|A|$.

Lemma 1.5. *If $A \subset \mathbb{R}$ is contained in an interval of the form $[x, 2x]$ for some $x > 0$, then*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{16/15}.$$

Proof. Write the elements of A as $a_1 < \cdots < a_{|A|}$. Set $s = \lfloor |A|^{1/5}/16 \rfloor$ and partition A into at least $8|A|^{4/5}$ sequences of the form $A_i = \{a_{(i-1)s+1}, \dots, a_{is}\}$ (omitting less than s elements of A). Let B be a set A_i that has the minimum value of $w = a_{is} - a_{(i-1)s+1}$.

We claim that if $j - i \geq 4$, then $A_i + B$ is disjoint from $A_j + B$, and $A_i \cdot B$ is disjoint from $A_j \cdot B$. For the first part, if $a \in A_i, a' \in A_j, b > b' \in B$, then $a' - a \geq 3w$ while $b - b' \leq w$, so we cannot have $a' - a = b - b'$, hence also not $a + b = a' + b'$. For the second part, again consider $a \in A_i, a' \in A_j, b > b' \in B$. We have $a'/a \geq (a + 3w)/a = 1 + 3w/a$ and $b/b' \leq (b' + w)/b' = 1 + w/b'$. By the assumption that $A \subset [x, 2x]$, we have $a \leq 2b'$, so

$3/a > 1/b'$. Thus $1 + 3w/a > 1 + w/b'$, which implies that we cannot have $a'/a = b/b'$, so also not $ab = a'b'$.

Let X_B be as in Lemma 1.4, so $|X_B| \leq |B|^4 \leq |A|^{4/5}$. Consider the sets A_{4i}, of which we have at least $2|A|^{4/5}$. It follows that at least $|A|^{4/5}$ of these sets are disjoint from X_B. Let I be the set of corresponding indices, so $|I| \geq |A|^{4/5}$ and for $i \in I$ we have

$$|B + A_{4i}| + |B \cdot A_{4i}| \gg |B|^{4/3} \gg |A|^{4/15}.$$

By the disjointness property observed above, we get

$$|A + A| + |A \cdot A| \geq \sum |B + A_{4i}| + |B \cdot A_{4i}| \gg |A|^{4/5} \cdot |A|^{4/15} = |A|^{16/15}.$$

This proves the lemma. □

Proof of Theorem 1.3. We can assume that all numbers in A are positive (if at least $|A|/3$ numbers in A are positive, we work only with those, while if at least $|A|/3$ numbers in A are negative, we multiply those by -1 and work with them, observing that $(-B) \cdot (-B) = B \cdot B$ and $|(-B) + (-B)| = |B + B|$ for any B).

We consider the "dyadic partition" of A into the sets

$$A_i = \{a \in A : 2^i < a \leq 2^{i+1}\}.$$

Note that for $i \neq j$, $A_i + A_i$ is disjoint from $A_j + A_j$, and $A_i \cdot A_i$ is disjoint from $A_j \cdot A_j$. Let I be the set of i for which $|A_i| \geq |A|^{15/31}$ or $|A_i| = 0$.

First suppose that $\sum_{i \in I} |A_i| \geq |A|/2$. For each $i \in I$, Lemma 1.5 gives

$$|A_i + A_i| + |A_i \cdot A_i| \gg |A_i|^{16/15} \gg |A_i| \cdot |A|^{1/31},$$

so we get

$$|A + A| + |A \cdot A| \geq \sum_{i \in I} |A_i + A_i| + |A_i \cdot A_i| \gg |A|^{1/31} \sum_{i \in I} |A_i| \gg |A|^{32/31},$$

and we are done.

Otherwise, we have $\sum_{i \notin I} |A_i| \geq |A|/2$, with each $|A_i|$ in this sum smaller than $|A|^{15/31}$, but nonzero. This implies that the number of terms in the sum is at least $|A|^{16/31}$. We can pick one element from each A_i, and let $B \subset A$ be the resulting set with $|B| \geq |A|^{16/31}$. Since each number of B is in a different dyadic interval, B has the property that for any three numbers in B, the largest is larger than the sum of the other two. Thus B has no distinct solutions of $b_1 + b_2 = b_3 + b_4$. This means that

$$|A + A| \geq |B + B| \gg |B|^2 \geq |A|^{32/31},$$

which completes the proof of the theorem. □

1.3 Convex sets and Elekes's improvement

In this section we show an improvement on Theorem 1.3 due to Elekes [3]. Elekes's proof used the Szemerédi–Trotter Theorem, and we will present it in the next chapter. Here we give a proof by Solymosi [23], which is more elementary in the sense that it does not use the Szemerédi–Trotter Theorem. Moreover, in the next chapter we will use it as inspiration for a proof of the Szemerédi–Trotter Theorem.

First we make a small detour to give a simpler version of Solymosi's argument, also from [23], which proves a related result.

We call $A = \{a_1 < \cdots < a_N\} \subset \mathbb{R}$ a *convex set* if each consecutive difference is larger than the previous consecutive difference, i.e. $a_{i+1} - a_i > a_i - a_{i-1}$. Hegyvári [9] proved that any convex set A satisfies $|A + A| \gg |A| \log |A| / \log\log |A|$, answering a question of Erdős. We show a much stronger bound of Elekes, Nathanson, and Ruzsa [4], which was originally proved using the Szemerédi–Trotter Theorem. Observe that a geometric progression is a convex set, so this is one way to generalize the observation that a geometric progression has a large sumset.

Theorem 1.6. *If $A = \{a_1 < a_2 < \cdots < a_{|A|}\} \subset \mathbb{R}$ is a convex set, then*

$$|A + A| \gg |A|^{3/2}.$$

Proof. We can split $\mathbb{R}$ into at most $|A|/2$ intervals, in such a way that each interval contains at most $4|A + A|/|A|$ elements of $A + A$. It does not matter if the intervals are open or closed. We can do this greedily by picking an interval containing the starting sequence of A of length $\lfloor 4|A + A|/|A| \rfloor$, then an interval containing the second such sequence, et cetera. Since $(|A|/2) \cdot \lfloor 4|A + A|/|A| \rfloor > |A + A|$, the number of resulting intervals is less than $|A|/2$.

Let X be the set of pairs (i, j) such that $a_i + a_j$ and $a_{i+1} + a_j$ lie in the same interval. For a fixed a_j, at most $|A|/2$ of the pairs $a_i + a_j, a_{i+1} + a_j$ can be separated, so at least $|A|/4$ are not separated, which gives

$$|X| \gg |A|^2.$$

On the other hand, each interval contains at most $4|A + A|/|A|$ elements of $A + A$. Two such elements $b < c \in A + A$ correspond to at most one pair $(i, j) \in X$, since if we have $b = a_i + a_j$ and $c = a_{i+1} + a_j$, then $c - b = a_{i+1} - a_i$, which by the convexity of A uniquely determines i. Thus we have

$$|X| \leq (|A|/2) \cdot \binom{4|A + A|/|A|}{2} \ll \frac{|A + A|^2}{|A|}.$$

Combining the lower and upper bound on X proves the theorem. □

Observe that the proof would still work if we replace convexity by the weaker assumption that the consecutive differences $a_{i+1} - a_i$ are all *distinct*. We could also easily prove that $|A + B| \gg |A||B|^{1/2}$ for an arbitrary set $B \subset \mathbb{R}$.

Schoen and Shkredov [20] obtained an improvement, which says that if A is convex, then $|A + A| \gg |A|^{14/9} \log^{-2/3} |A|$, as well as $|A - A| \gg |A|^{8/5} \log^{-2/5} |A|$.

We now give a two-dimensional version of the proof above, which leads to a sum-product bound that is better than Theorem 1.3.

We can think of two sequences $a_1 < \cdots < a_N$ and $c_1 < \cdots < c_N$ of the same length, such that the points (a_i, c_i) form a convex set in $\mathbb{R}^2$, i.e., the consecutive difference vectors $(a_{i+1}, c_{i+1}) - (a_i, c_i)$ have increasing slopes. But, much like in the previous theorem, all we need for the proof is that the consecutive differences between these points are distinct, and we state the theorem with that condition.

Theorem 1.7. *Let $A = \{a_1 < a_2 < \cdots < a_N\} \subset \mathbb{R}$ and $C = \{c_1 < c_2 < \cdots < c_N\} \subset \mathbb{R}$. Assume that all consecutive difference vectors $(a_{i+1} - a_i, c_{i+1} - c_i)$ are distinct. Then for any $B, D \subset \mathbb{R}$ we have*

$$|A + B| \cdot |C + D| \gg (N^3|B||D|)^{1/2}.$$

Proof. We partition $\mathbb{R}^2$ into cells using a procedure like that in the proof of Theorem 1.6. On the x-axis we partition $\mathbb{R}$ into at most $N/4$ intervals, each containing at most $8|A + B|/N$ elements of $A + B$, and on the y-axis we partition $\mathbb{R}$ into at most $N/4$ intervals, each containing at most $8|C + D|/N$ elements of $C + D$. Combining these partitions gives a partition of $\mathbb{R}^2$ into at most $N^2/16$ cells, each of which contains at most $64|A+B||C+D|/N^2$ points of $(A + B) \times (C + D)$.

Let X be the set of triples $(i, b, d) \in [N] \times B \times D$ such that the points

$$(a_i + b, c_i + d) \text{ and } (a_{i+1} + b, c_{i+1} + d)$$

lie in the same cell.

For a fixed $b \in B$ and $d \in D$, at most $N/4$ points $(a_i + b, c_i + d)$ are separated from $(a_{i+1} + b, c_{i+1} + d)$ by a vertical cut, and at most $N/4$ by a horizontal cut, so at least $N/4$ pairs are not separated. Thus

$$X \gg N|B||D|.$$

On the other hand, each cell contains at most $64|A + B||C + D|/N^2$ points of $(A + B) \times (C + D)$, and by the assumption that the successive difference vectors are distinct, any pair of those points corresponds to at most one triple $(i, b, d) \in X$. Hence

$$|X| \leq (N^2/16) \cdot \binom{64|A + B||C + D|/N^2}{2} \ll \frac{|A + B|^2|C + D|^2}{N^2}.$$

Combining the lower and upper bound on X proves the theorem. □

Corollary 1.8 (Elekes). *For $A \subset \mathbb{R}$ we have*

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

and thus

$$\max\{|A + A|, |A \cdot A|\} \gg |A|^{5/4}.$$

Proof. We can assume that the numbers in A are positive (as in the proof of Theorem 1.3). Apply Theorem 1.7 with $A = B, C = D = \log(A) = \{\log(a) : a \in A\}$. Writing $A = \{a_1 < \cdots < a_N\}$ and $C = \{c_1 < \cdots < c_n\}$, the points (a_i, c_i) lie on the graph $y = \log(x)$. Since the logarithm is a convex function, it follows that the difference vectors $(a_{i+1} - a_i, c_{i+1} - c_i)$ are distinct. □

Corollary 1.9. *For $A \subset \mathbb{R}$ we have*

$$|A + A^2| \gg |A|^{5/4}.$$

Proof. Apply Theorem 1.7 with $B = A^2, C = A^2, D = A$. The distinct difference vector property follows from the fact that the function x^2 is concave. □

Note that this also implies $|A + A \cdot A| \gg |A|^{5/4}$, since $A^2 \subset A \cdot A$.

1.4 Solymosi's bound

In this section we give an even better sum-product bound, due to Solymosi [26]. Again we introduce the argument in an easier case, by proving that either the sumset is large or the *quotientset* $A/A = \{a/b : a, b \in A, b \neq 0\}$ is large. This version of Solymosi's argument was given by Li and Shen [14].

Theorem 1.10. *If $A \subset \mathbb{R}$, then*

$$|A + A|^2 |A/A| \gg |A|^4,$$

and thus

$$\max\{|A + A|, |A/A|\} \gg |A|^{4/3}.$$

Proof. We can assume that all numbers in A are positive. The Cartesian product $A \times A$ is covered by the lines through the origin with slopes from A/A. Label these lines $L_1, L_2, \ldots$ in order of increasing slope. The following observation is crucial: If for $i \neq j$ we add the points of $A \times A$ on L_i to the points of $A \times A$ on L_j, then we get

$$|L_i \cap (A \times A)| \cdot |L_j \cap (A \times A)|$$

distinct points of

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

Moreover, these points lie in the sector between the two lines, so if we do this for pairs of lines whose sectors do not overlap, then we get all distinct points. Therefore, for any subset $i_1 < i_2 < \cdots < i_k$ of the indices of the lines, we have

$$\sum_{j=1}^{k-1} |L_{i_j} \cap (A \times A)| \cdot |L_{i_{j+1}} \cap (A \times A)| \leq |A + A|^2.$$

Let $i_1 < i_2 < \cdots < i_k$ be the indices of the lines that contain at least $|A|^2/(2|A/A|)$ points of $A \times A$. Since the other lines contain less than $|A/A| \cdot |A|^2/(2|A/A|) = |A|^2/2$ points of $A \times A$, and since $|L_{i_k} \cap (A \times A)| \leq |A| \leq |A|^2/4$, we have

$$\sum_{j=1}^{k-1} |L_{i_j} \cap (A \times A)| \geq |A|^2/4.$$

Hence

$$|A + A|^2 \geq \sum_{j=1}^{k-1} |L_{i_j} \cap (A \times A)| \cdot |L_{i_{j+1}} \cap (A \times A)| \geq \frac{|A|^2}{2|A/A|} \sum_{j=1}^{k-1} |L_{i_j} \cap (A \times A)| \gg \frac{|A|^4}{|A/A|}.$$

This proves the theorem. □

Theorem 1.11. *If $A \subset \mathbb{R}$, then*

$$|A+A|^2|A\cdot A| \gg \frac{|A|^4}{\log|A|},$$

and thus

$$\max\{|A+A|,|A\cdot A|\} \gg \frac{|A|^{4/3}}{\log^{1/3}|A|}.$$

Proof. Again we cover $A\times A$ by lines $L_1, L_2, \ldots$, ordered by increasing slope. As in the proof of Theorem 1.10, for any subset $i_1 < \cdots < i_k$ of the indices, we have

$$\sum_{j=1}^{k-1} |L_{i_j} \cap (A\times A)||L_{i_{j+1}} \cap (A\times A)| \le |A+A|^2. \tag{1.1}$$

We define

$$E = \{(a,b,c,d) \in A^4 : ab = cd\}.$$

On the one hand, using the Cauchy-Schwarz inequality we have

$$\begin{aligned} |E| &= \sum_{p\in A\cdot A} |\{(a,b)\in A^2 : ab = p\}|^2 \\ &\ge \frac{1}{|A\cdot A|}\left(\sum_{p\in A\cdot A} |\{(a,b)\in A^2 : ab=p\}\right)^2 \ge \frac{|A|^4}{|A\cdot A|}. \end{aligned} \tag{1.2}$$

On the other hand, we have

$$\begin{aligned} |E| &= |\{(a,b,c,d)\in A^4 : a/d = c/b\}| \\ &= \sum_{q\in A/A} |\{(a,d)\in A^2 : a/d = q\}|^2 = \sum_{i\ge 1} |L_i\cap(A\times A)|^2. \end{aligned}$$

To obtain an upper bound using (1.1), we need to choose a subset of the indices for which $|L_i\cap(A\times A)|^2$ is comparable to $|L_{i_j}\cap(A\times A)||L_{i_{j+1}}\cap(A\times A)|$. We can do that by dyadically splitting the sum of squares as

$$\sum_{j=0}^{\lceil \log|A|\rceil} \sum_{2^j \le |L_i\cap(A\times A)| < 2^{j+1}} |L_i\cap(A\times A)|^2,$$

so by the pigeonhole principle there is an integer J such that

$$\frac{|E|}{\lceil\log|A|\rceil} \le \sum_{2^J\le|L_i\cap(A\times A)|<2^{J+1}} |L_i\cap(A\times A)|^2.$$

Let $i_1 < \cdots < i_k$ be the indices of the lines L_{i_j} for which $2^J \le |L_{i_j}\cap(A\times A)| < 2^{J+1}$, so that $|L_{i_j}\cap(A\times A)| \le 2|L_{i_{j+1}}\cap(A\times A)|$ for every j. This also allows us to leave out the term in the sum involving L_{i_k}, since we have $|L_{i_k}\cap(A\times A)|^2 \le 4|L_{i_1}\cap(A\times A)|^2$ and we can adjust the implicit constant (if $k=1$ we can use $|L_{i_k}\cap(A\times A)|^2 \le |A|^2 \le |A+A|^2$). Therefore, we have

$$\frac{|E|}{\log|A|} \ll \sum_{j=1}^{k-1} |L_{i_j}\cap(A\times A)|^2 \ll \sum_{j=1}^{k-1} |L_{i_j}\cap(A\times A)||L_{i_{j+1}}\cap(A\times A)| \le |A+A|^2.$$

Together with (1.2) this finishes the proof. □

Chapter 2

Sum-product bounds via incidence geometry

2.1 The Szemerédi–Trotter Theorem

Given a set P of points and a set L of lines, we define

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

We give an elementary proof of a special case of a theorem of Szemerédi and Trotter [27], which uses the same partitioning idea as the proof that we gave for Theorem 1.7.

Theorem 2.1. *Let $A, B \subset \mathbb{R}$, set $P = A \times B \subset \mathbb{R}^2$, and let L be a set of lines in $\mathbb{R}^2$. Assume that $|A| \leq |B|$ and $|B|^2/|A| \leq |L| \leq |A|^2|B|^2$. Then*

$$|I(P, L)| \ll |A|^{2/3}|B|^{2/3}|L|^{2/3}.$$

Proof. Let r be a parameter that we will choose at the end of the proof. We cut $\mathbb{R}$ at $r-1$ points so that each of the r resulting intervals contains at most $2|A|/r$ numbers from A, and similarly we cut $\mathbb{R}$ into r intervals containing at most $2|B|/r$ numbers from B. Combining these two partitions gives a partition of $\mathbb{R}^2$ into r^2 cells, each of which contains at most $4|A||B|/r^2 = 4|P|/r^2$ points of $P = A \times B$. We can this for any r satisfying $1 \leq r \leq |A|$.

An important observation is that a line intersects at most $2r$ of the r^2 cells, since to pass from one cell to another, a line has to cross one of the $r-1$ vertical cutting lines or one of the $r-1$ horizontal cutting lines, and it intersects each of those line at most once (unless the line is itself a cutting line, but then it does not contain any points of P).

Let I_1 be the set of incidences $(p, \ell) \in I(P, L)$ such that (p, ℓ) is the only incidence involving ℓ in the cell that p is in, and let I_2 be the set of incidences $(p, \ell) \in I(P, L)$ such that ℓ has at least two incidences with P in the cell containing p. Since a line intersects at most $2r$ cells, we have

$$|I_1| \leq 2r \cdot |L| \ll r|L|.$$

A cell contains at most $4|P|/r^2$ points of P, so it contains at most $\binom{4|P|/r^2}{2}$ pairs of points. Each pair of points in a cell lies on at most one line of L, so it contributes at most two incidences to I_2. Hence in each of the r^2 cells there are at most $2 \cdot \binom{4|P|/r^2}{2}$ incidences of I_2, so

$$|I_2| \leq r^2 \cdot 2 \cdot \binom{4|P|/r^2}{2} \ll \frac{|P|^2}{r^2}.$$

Altogether we have

$$|I(P,L)| \le |I_1| + |I_2| \ll r|L| + \frac{|P|^2}{r^2}.$$

To minimize this upper bound, we equate $r|L| = |P|^2/r^2$, which leads us to $r = \lfloor |P|^{2/3}/|L|^{1/3} \rfloor$. The resulting bound is the one in the theorem. For the partitioning step to work, we need $1 \le r \le |A|$, or equivalently $|L|^{1/3} \le |A|^{2/3}|B|^{2/3} \le |A||L|^{1/3}$, which is equivalent to the assumption in the theorem. □

The following construction shows that this bound is tight. For any positive integers $a \le b$ with a dividing b, we take

$$P = [a] \times [b], \quad L = \{y = sx + t : s \in [b/a], t \in [b]\},$$

so that $|P| = ab$ and $|L| = b^2/a$. For every $s \in [b/(2a)]$ and $t \in [b/2]$ the line $y = sx + t$ contains $(i, si + t) \in P$ for every $i \in [a]$, so

$$|I(P,L)| \ge \frac{b}{2a} \cdot \frac{b}{2} \cdot a \gg b^2.$$

On the other hand, we have $b^2/a \le |L| \le a^2b^2$, so Theorem 2.1 gives

$$|I(P,L)| \ll a^{2/3}b^{2/3}(b^2/a)^{2/3} = b^2.$$

The following corollary more closely resembles the original formulation of Szemerédi and Trotter [27] (which gives the bound in Corollary 2.2 for an arbitrary point set P).

Corollary 2.2. *Let $A, B \subset \mathbb{R}$ with $|A| = |B|$, set $P = A \times B \subset \mathbb{R}^2$, and let L be a set of lines in $\mathbb{R}^2$. Then*

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

Proof. First suppose that $|P|^{1/2} \le |L| \le |P|^2$. This implies $|B|^2/|A| \le |L| \le |A|^2|B|^2$, so we can apply Theorem 2.1 to get $|I(P,L)| \ll |P|^{2/3}|L|^{2/3}$.

Suppose $|P|^{1/2} > |L|$. The points of P that are incident to at most one line of L give at most $|P|$ incidences. Every other point of P is an intersection point of at least two lines of L. Any two lines of L have at most one intersection point, so the number of incidences involving intersection points is at most $|L|^2 \le |P|$.

Finally, suppose $|L| > |P|^2$. The lines of L containing at most one point of P together give at most $|L|$ incidences. Every other line of L is spanned by at least two points of P. Any two points of P span at most one such line, so the number of incidences involving lines spanned by P is at most $|P|^2 \le |L|$. □

2.2 Applications to sum-product bounds

We can now use Theorem 2.1 to reprove Corollary 1.8, which is Elekes's sum-product bound [3]. This is essentially Elekes's original proof, although Elekes used the original Szemerédi–Trotter Theorem [27].

Theorem 2.3 (Elekes). *For $A \subset \mathbb{R}$ we have*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{5/4}.$$

Proof. Define a point set

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

and a line set

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

On the one hand, every line in L contains at least $|A|$ points of A, since $(a+c, bc)$ satisfies $y = b(x-a)$ for every $c \in A$. Thus $|I(P,L)| \geq |A| \cdot |L| = |A|^3$.

We apply Theorem 2.1. The condition $|L| \leq |P|^2$ clearly holds. If we let M be the larger one of $|A+A|$ and $|A \cdot A|$, and N the smaller one, then the condition of Theorem 2.1 is $M^2/N \leq |L| \leq M^2N^2$. We clearly have $|L| = |A|^2 \leq M^2N^2$. If the condition $|L| \geq M^2/N$ does not hold, then we have $|A|^2 < M^2/N$, so $M > |A|N^{1/2} \geq |A|^{3/2}$, and we are done. Thus we can assume that both conditions hold and we can apply Theorem 2.1. We get

$$|A|^3 \leq |I(P,L)| \ll |A+A|^{2/3}|A \cdot A|^{2/3}(|A|^2)^{2/3},$$

which gives $|A+A||A \cdot A| \gg |A|^{5/2}$ and proves the theorem. □

We prove several other consequences of Theorem 2.1. The first is a lower bound for the size of the expression $A + B \cdot C$. This question was first considered over finite fields by Barak, Impagliazzo, and Wigderson [2]. The observation that over $\mathbb{R}$ a good bound can be obtained using the Szemerédi–Trotter Theorem was first recorded by Tao and Vu [28, Exercise 8.3.3], as well as by Alon and Spencer [1, p. 287, Theorem 3]. Remarkable, there has been no improvement to this simple bound, even in the case of $A + A \cdot A$.

Theorem 2.4. *For $A, B, C \subset \mathbb{R}$ not equal to $\{0\}$ we have*

$$|A + B \cdot C| \gg |A|^{1/2}|B|^{1/2}|C|^{1/2}.$$

In particular, we have $|A + A \cdot A| \gg |A|^{3/2}$ and $|A \cdot A + A \cdot A| \gg |A|^{3/2}$.

Proof. Define

$$P = C \times (A + B \cdot C), \quad L = \{y = a + bx : a \in A, b \in B\}.$$

Every line of L contains exactly $|C|$ points of P, namely the points $(c, a+bc)$ for $c \in C$, so we have $|I(P,L)| = |A||B||C|$.

The first condition of Theorem 2.1 is that $|C| \leq |A + B \cdot C|$. Since $B \neq \{0\}$, we can pick a nonzero $b \in B$ to get

$$|A + B \cdot C| \geq |A + bC| \geq |C|.$$

The second condition of Theorem 2.1 is $|A + B \cdot C|^2/|C| \leq |A||B| \leq |C|^2|A + B \cdot C|^2$. If the first inequality does not hold, then we get the bound in the theorem directly. For the second inequality, we can pick a nonzero $c \in C$ to get

$$|A + B \cdot C| \geq |A + cB| \geq \max\{|A|, |B|\} \geq (|A||B|)^{1/2}.$$

Thus

$$|A||B||C| = |I(P,L)| \ll |C|^{2/3}|A + B \cdot C|^{2/3}(|A||B|)^{2/3}.$$

Rearranging completes the proof. □

The next application of Theorem 2.1 is an expansion bound for a two-variable polynomial, which in general is harder to obtain than an expansion bound for a three-variable polynomial like $x + yz$. This result was first obtained by Raz, Sharir, and Solymosi [15], but similar proofs can be found in Hegyvári and Hennecart [10] and Sharir, Sheffer, and Solymosi [22].

Theorem 2.5. *Let $f(x,y) = x^2 + xy$. For $A \subset \mathbb{R}$ we have*

$$|f(A,A)| \gg |A|^{4/3}.$$

Proof. Define

$$E = \{(a,b,c,d) \in A^4 : f(a,b) = f(c,d)\}.$$

Using the Cauchy-Schwarz inequality we have

$$\begin{aligned} |E| &= \sum_{e \in f(A,A)} |\{(a,b) \in A^2 : f(a,b) = e\}|^2 \\ &\geq \frac{1}{|f(A,A)|} \left(\sum_{e \in f(A,A)} |\{(a,b) \in A^2 : f(a,b) = e\}| \right)^2 = \frac{|A|^4}{|f(A,A)|}. \end{aligned}$$

On the other hand, we have

$$|E| = \sum_{(s,t) \in A^2} |\{(x,y) \in A^2 : f(s,x) = f(t,y)\}|, \tag{2.1}$$

and we can observe that $f(a,b) = f(c,d)$ is a linear equation in b and d.

We define

$$P = A \times A, \quad L = \{f(s,x) = f(t,y) : s,t \in A\}.$$

The equation $f(s,x) = f(t,y)$ is equivalent to $sx - ty = t^2 - s^2$, which is linear in x and y, so L is a set of lines. Any $(s,t) \in A \times A$ with $s \neq \pm t$ gives a distinct line. The lines with $s = \pm t$ may have multiplicity, but there are at most $2|A|$ such pairs, each of which contributes at most $|A|$ to the sum (2.1). Thus we have $|E| \ll |I(P,L)|$.

Applying Theorem 2.1 (the condition $|A| \leq |L| \leq |A|^4$ clearly holds), we get

$$|E| \ll |I(P,L)| \ll |A|^{2/3}|A|^{2/3}(|A|^2)^{2/3} \ll |A|^{8/3}.$$

Combining this with $|f(A,A)| \geq |A|^4/|E|$ proves the theorem. □

Finally, we give a more intricate application of Theorem 2.1. The result was first proved by Roche-Newton and Rudnev [17], but the more elementary proof that we give was found by Roche-Newton [16].

Theorem 2.6. *For $A \subset \mathbb{R}$ we have*

$$|(A-A)(A-A)| \gg \frac{|A|^2}{\log |A|}.$$

Proof. Define

$$F(x,y,z) = \frac{(x-y)}{(x-z)}$$

and

$$E = \{(a,b,c,a',b',c') \in A^6 : F(a,b,c) = F(a',b',c')\}.$$

Observe that $F(a,b,c) = F(a',b',c')$ is equivalent to

$$\frac{a-b}{a'-b'} = \frac{a-c}{a'-c'},$$

which means that the point $(a,a'),(b,b'),(c,c')$ are collinear.

Let L be the set of all lines determined by $A \times A$. Then we have

$$|E| \leq \sum_{\ell \in L} |\ell \cap (A \times A)|^3.$$

We can dyadically decompose this sum, with $L_j = \{\ell \in L : 2^j \leq |\ell \cap (A \times A)| < 2^{j+1}\}$, as

$$\sum_{j=1}^{\lfloor \log |A| \rfloor} \sum_{\ell \in L_j} |\ell \cap (A \times A)|^3.$$

By Theorem 2.1, we have $2^j |L_j| \ll |A|^{2/3} |A|^{2/3} |L_j|^{2/3}$, which gives $|L_j| \ll |A|^4 / 2^{3j}$ (the condition of Theorem 2.1 is $|A| \leq |L_j| \leq |A|^4$; the second inequality is clear, and if the first fails, we have $|L_j| \leq |A| \ll |A|^4/2^{3j}$ anyway). Thus

$$|E| \ll \sum_{j=1}^{\lfloor \log |A| \rfloor} \frac{|A|^4}{2^{3j}} \cdot (2^{j+1})^3 \ll |A|^4 \log |A|.$$

We can rewrite $|E|$ to

$$|E| = \sum_{(a,a') \in A^2} |\{(b,c,b',c') \in A^4 : (a-b)(a'-c') = (a-c)(a'-b'),\}|$$

so there must be some $(a_0, a_0') \in A^2$ such that

$$|\{(b,c,b',c') \in A^4 : (a_0-b)(a_0'-c') = (a_0-c)(a_0'-b')\}| \ll |A|^2 \log |A|.$$

Write $G(x,y) = (a_0 - x)(a_0' - y)$. By the above and the Cauchy-Schwarz inequality we have

$$\begin{aligned} |A|^2 \log |A| &\gg \sum_{g \in G(A,A)} |\{(b,c') \in A^2 : G(b,c') = g\}|^2 \\ &\geq \frac{1}{|G(A,A)|} \left(\sum_{g \in G(A,A)} |\{(b,c') \in A^2 : G(b,c') = g\}| \right)^2 = \frac{|A|^4}{|G(A,A)|}. \end{aligned}$$

Since $G(A,A) \subset (A-A)(A-A)$, this proves the desired bound. □

Chapter 3

Sum-product bounds in finite fields

3.1 Introduction

In this chapter we study sum-product bounds in finite fields $\mathbb{F}_p$ and $\mathbb{F}_q$ (where p is a prime and q is a prime power). The first observation to make is that if A is a subfield (or the field itself), then we have $\max\{|A+A|, |A\cdot A|\} = |A|$. Therefore, any interesting sum-product bound over finite fields must have some condition on A that precludes A from being a subfield.

Moreover, the following observation shows that even for sets that are far from being subfields, it cannot be true that $\max\{|A+A|, |A\cdot A|\} \gg |A|^{2-\epsilon}$, unlike what is conjectured in $\mathbb{R}$.

Proposition 3.1. *For any prime q and any $N \leq q$ there is a set $A \subset \mathbb{F}_q$ with $|A| = N$ and*

$$\max\{|A+A|, |A\cdot A|\} \ll q^{1/2}|A|^{1/2}.$$

In particular, there is a set $A \subset \mathbb{F}_q$ with $|A| \approx q^{1/2}$ such that $\max\{|A+A|, |A\cdot A|\} \ll |A|^{3/2}$.

Proof. It is a standard result from algebra that $\mathbb{F}_q^*$ is a cyclic group, i.e., there is a generator $g \in \mathbb{F}_q^*$ such that $\mathbb{F}_q^* = \{g^i : i \in [q-1]\}$. For any $M \leq q-1$ we have

$$\sum_{t\in\mathbb{F}_q} \left|\{g^i : i \in [M]\} \cap ([M]+t)\right| = M^2,$$

since each pair $i, j \in [M]$ is counted exactly once in the sum, in the term for $t = g^i - j$. By the pigeonhole principle, there exists a t_0 such that

$$\left|\{g^i : i \in [M]\} \cap ([M]+t_0)\right| \geq \frac{M^2}{q}.$$

Given N, set $M = \lceil q^{1/2}N^{1/2}\rceil$, so we can pick a set $A \subset \{g^i : i \in [M]\} \cap ([M]+t_0)$ with $|A| = N$. Then we have $|A\cdot A| \leq 2M$ since $A \subset \{g^i : i \in [M]\}$, and we have $|A+A| \leq 2M$ since $A \subset [M]+t_0$. □

In the next section we show that this bound is tight for $|A| \geq q^{2/3}$, and after that we will see weaker bounds for smaller sets. In both cases, the bounds rely on point-line incidence bounds analogous to Theorem 2.1.

3.2 Sum-product bounds for large subsets of finite fields

We can obtain a strong incidence bound for "large" sets of points and lines, by which we roughly mean sets of size at least q. The bound is due to Vinh [29], and we give a simplified proof due to Murphy and Petridis [13].

To be precise, a *line* in $\mathbb{F}_q^2$ is a solution set of a linear equation. We use the following basic facts: A line in $\mathbb{F}_q^2$ contains exactly q points, a point in $\mathbb{F}_q^2$ lies on exactly $q+1$ lines, and the number of lines in $\mathbb{F}_q^2$ is q^2+q.

Theorem 3.2 (Vinh). *For a point set $P \subset \mathbb{F}_q^2$ and a line set L in $\mathbb{F}_q^2$ we have*

$$\left| |I(P,L)| - \frac{|P||L|}{q} \right| \leq q^{1/2}|P|^{1/2}|L|^{1/2}.$$

Proof. Let M be the set of all lines in $\mathbb{F}_q^2$. Using the triangle inequality and the Cauchy-Schwarz inequality we have

$$\begin{aligned}\left| |I(P,L)| - \frac{|P||L|}{q} \right| &= \left| \sum_{\ell \in L} \left(|\ell \cap P| - \frac{|P|}{q} \right) \right| \leq \sum_{\ell \in L} \left| |\ell \cap P| - \frac{|P|}{q} \right| \\ &\leq \left(|L| \sum_{\ell \in L} \left(|\ell \cap P| - \frac{|P|}{q} \right)^2 \right)^{1/2} \leq \left(|L| \sum_{\ell \in M} \left(|\ell \cap P| - \frac{|P|}{q} \right)^2 \right)^{1/2}.\end{aligned}$$

The sum of squares expands as

$$\sum_{\ell \in M} \left(|\ell \cap P| - \frac{|P|}{q} \right)^2 = \sum_{\ell \in M} |\ell \cap P|^2 - \frac{2|P|}{q} \sum_{\ell \in M} |\ell \cap P| + \frac{|M||P|^2}{q^2}.$$

As mentioned above, we have $|M| = q^2+q$, and every point in $\mathbb{F}_q^2$ lies on exactly $q+1$ lines of M, which implies

$$\sum_{\ell \in M} |\ell \cap P| = (q+1)|P|.$$

Using this equality and the fact that any two distinct points determine one line, we have

$$\begin{aligned}\sum_{\ell \in M} |\ell \cap P|^2 &= \sum_{\ell \in M} |\{(p,p') \in (\ell \cap P)^2 : p \neq p'\}| + \sum_{\ell \in M} |\{(p,p') \in (\ell \cap P)^2 : p = p'\}| \\ &= |\{(p,p') \in P^2 : p \neq p'\}| + \sum_{\ell \in M} |\ell \cap P| \\ &= |P|(|P|-1) + (q+1)|P| \\ &= q|P| + |P|^2.\end{aligned}$$

Altogether, we get

$$\sum_{\ell \in M} \left(|\ell \cap P| - \frac{|P|}{q} \right)^2 = q|P| + |P|^2 - \frac{2|P|}{q} \cdot (q+1)|P| + \frac{|P|^2 \cdot q(q+1)}{q^2} = q|P| - \frac{|P|^2}{q}.$$

Bounding this by $q|P|$, we get

$$\left| |I(P,L)| - \frac{|P||L|}{q} \right| \leq \left(|L| \cdot q|P| \right)^{1/2},$$

which completes the proof. □

To get some feeling for the bound, observe that if $|P| = |L| = N$, then for $N \gg q^{3/2}$ the bound gives $|I(P,L)| \approx N^2/q$, while for $N \ll q^{3/2}$ it is $|I(P,L)| \ll q^{1/2}N$. Remarkably, for $N \approx q^{3/2}$ it is $|I(P,L)| \ll N^{4/3}$, which is the same exponent as in the Szemerédi–Trotter Theorem (see Theorem 2.1).

In the upper range $N \gg q^{3/2}$, the bound is clearly tight (up to constants), since it gives its own lower bound. The lower range $N \ll q^{3/2}$ is more subtle. If for instance $q = p^2$, then we can take $P = \mathbb{F}_p^2 \subset \mathbb{F}_q^2$ and $L = \{y = ax + b : a, b \in \mathbb{F}_p\}$, which gives $N = q$ and $|I(P,L)| \approx N^{3/2}$. For $q \leq N \leq q^{3/2}$, we can take N/q disjoint translated copies of this construction, so that $|P| = |L| = N$ and $|I(P,L)| \approx q^{1/2}N$ (since each of the N lines contains $p = q^{1/2}$ points of P).

Just as we used the Szemerédi–Trotter incidence bound to prove a sum-product bound in Theorem 2.3, we can now use Theorem 3.2 in to obtain a sum-product bound for "large" subsets of finite fields (where "large" now roughly means sets of size more than $q^{1/2}$). This bound was first proved by Garaev [6] using different methods, but Vinh [29] observed that it can also be proved via the incidence bound above.

Corollary 3.3 (Garaev). *For $A \subset \mathbb{F}_q$ with $q^{2/3} \leq |A| \leq q$ we have*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{1/2}q^{1/2},$$

and for $A \subset \mathbb{F}_q$ with $q^{1/2} \leq |A| \leq q^{2/3}$ we have

$$\max\{|A+A|, |A \cdot A|\} \gg \frac{|A|^2}{q^{1/2}}.$$

Proof. As in the proof of Theorem 2.3, we define

$$P = (A+A) \times (A \cdot A), \quad L = \{y = b(x-a) : a, b \in A\}.$$

Since $(a+c, bc) \in P$ satisfies $y = b(x-a)$ for all $c \in A$, each line in L contains at least $|A|$ points of P, so we have $|I(P,L)| \geq |A||L| = |A|^3$. By Theorem 3.2 we have

$$|A|^3 \leq |I(P,L)| \leq \frac{|P||L|}{q} + q^{1/2}|P|^{1/2}|L|^{1/2} = \frac{|A+A||A \cdot A||A|^2}{q} + q^{1/2}|A+A|^{1/2}|A \cdot A|^{1/2}|A|.$$

If the first term dominates, then we have $|A+A||A \cdot A| \gg q|A|$, and if the second term dominates we have $|A+A||A \cdot A| \gg |A|^4/q$. Comparing these bounds gives the statement in the theorem. □

The tightness of these bounds is much like that of Theorem 3.2. The bound in the upper range $|A| \geq q^{2/3}$ is tight (up to constants) by Proposition 1.1. For $|A| \approx q^{2/3}$, the bound is $\max\{|A+A|, |A \cdot A|\} \gg |A|^{5/4}$, just as in Theorem 2.3. If $q = p^2$, then taking $A = \mathbb{F}_p \subset \mathbb{F}_q$ gives $\max\{|A+A|, |A \cdot A|\} = p = |A|^2/q^{1/2}$. However, if $q = p$, we will see in the next section that we can do better.

The next few corollaries give analogues of some of the corollaries in Section 2.2, using similar arguments.

Corollary 3.4. *For $A \subset \mathbb{F}_q$ with $q^{2/3} \leq |A| \leq q$ we have*

$$|A + A \cdot A| \gg q,$$

and for $A \subset \mathbb{F}_q$ with $q^{1/2} \leq |A| \leq q^{2/3}$ we have

$$|A + A \cdot A| \gg \frac{|A|^3}{q}.$$

Proof. As in the proof of Theorem 2.4, we define

$$P = A \times (A + A \cdot A), \quad L = \{y = a + bx : a, b \in A\}.$$

By Theorem 3.2 we get

$$|A|^3 = |I(P, L)| \leq \frac{|A|^3 |A + A \cdot A|}{q} + q^{1/2} |A|^{3/2} |A + A \cdot A|^{1/2}.$$

The first term gives $|A + A \cdot A| \gg q$, and the second gives $|A + A \cdot A| \gg |A|^3/q$. □

Corollary 3.5. *Let $f(x, y) = x^2 + xy$. For $A \subset \mathbb{F}_q$ we have*

$$|f(A, A)| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

Proof. We define

$$P = A \times A, \quad L = \{f(s, x) = f(t, y) : s, t \in A\}.$$

As in the proof of Theorem 2.5 we have

$$|f(A, A)| \geq \frac{|A|^4}{|I(P, L)|}.$$

Theorem 3.2 gives

$$|I(P, L)| \leq \frac{|A|^4}{q} + q^{1/2} |A|^2.$$

This leads to the bound in the theorem. □

The following statement is due to Hieu and Vinh [11].

Corollary 3.6. *For $A, B, C \subset \mathbb{F}_q$ we have*

$$|(A - B)^2 + C| \gg \min\left\{q, \frac{|A||B||C|}{q}\right\}.$$

In particular, we have $|(A - A)^2 + (A - A)^2| \gg \min\{q, |A|^3/q\}$.

Proof. We define

$$P = A \times ((A - B)^2 + C), \quad C = \{y = (x - b)^2 + c : b \in B, c \in C\}.$$

The curves in C are parabolas and not lines, but we can apply the transformation $\varphi : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ defined by

$$\varphi(x, y) = (x, y - x^2).$$

This is a bijection, so it preserves incidences, and it maps a point (x, y) on a parabola of the form $y = x^2 + sx + t$ to the point (u, v) on the line $v = su + t$. Thus $\varphi(C)$ is a set of lines, and $|I(\varphi(P), \varphi(C))| = |I(P, C)|$. Thus we have

$$\begin{aligned} |A||B||C| &\ll \frac{|\varphi(P)||\varphi(C)|}{q} + q^{1/2}(|\varphi(P)||\varphi(C)|)^{1/2} \\ &= \frac{|A||B||C||(A - B)^2 + C|}{q} + q^{1/2}(|A||B||C||(A - B)^2 + C|)^{1/2}, \end{aligned}$$

which gives the bound in the statement. □

The following bound is due to Solymosi [25].

Corollary 3.7. *For $A \subset \mathbb{F}_q$ we have*

$$|A + A^2| \gg \min\left\{q^{1/2}|A|^{1/2}, \frac{|A|^2}{q}\right\}.$$

Proof. We define

$$P = (A + A^2) \times (A + A^2), \quad C = \{y = (x - a^2)^2 + b : a, b \in A\}.$$

Using the same trick as in the proof of Corollary 3.6 to turn these parabolas into lines, we can apply Theorem 3.2 to get

$$|A|^3 \leq \frac{|A + A^2|^2|A|^2}{q} + q^{1/2}|A + A^2||A|,$$

which gives the stated bound. □

3.3 A point-line incidence bound over arbitrary fields

Let $\mathbb{F}$ be an arbitrary field with characteristic p. We make the convention that if $\mathbb{F}$ has characteristic zero, then $p = \infty$; this is convenient in some of the statements below, for instance because it makes a condition like $|A||L| \leq p^2$ vacuous in characteristic zero.

Theorem 3.2 states a point-line incidence bound that applies to large subsets of finite fields, but gives no information for smaller subsets. The following point-line incidence bound applies also to small subsets of finite fields, and in fact the proof works over arbitrary fields, but with a condition that the sets involved are relatively small compared to the characteristic. The bound was proved by Stevens and De Zeeuw [24], based on results of Rudnev [19] and Guth and Katz [7]. The proof involves some concepts from algebraic geometry that are outside the scope of this course, but we present most of the proof in this section. In the next section we deduce some sum-product bounds.

Theorem 3.8. *Let $A, B \subset \mathbb{F}$, set $P = A \times B \subset \mathbb{F}^2$, and let L be a set of lines in $\mathbb{F}^2$. Assume that $|A| \leq |B|$, that $|B|^2/|A| \leq |L| \leq |A||B|^2$, and that $|A||L| \leq p^2$. Then*

$$|I(P, L)| \ll |A|^{3/4}|B|^{1/2}|L|^{3/4}.$$

Note that the condition $|B|^2/|A| \leq |L| \leq |A||B|^2$ is almost identical to the condition on $|L|$ in Theorem 2.1. For $|L|$ outside this range, a simple combinatorial argument gives the better bound $|I(P, L)| \ll \min\{|P|^{1/2}|L| + |P|, |P||L|^{1/2} + |L|\}$, but inside the stated range of $|L|$, Theorem 3.8 is stronger than this combinatorial bound.

The condition $|A||L| \leq p^2$ keeps the statement away from subfields; specifically, it excludes cases like $A = B = \mathbb{F}_p$ and L being the set of all lines in $\mathbb{F}_p^2$, in which case we would have $|I(P, L)| = p^3$, whereas $|A|^{3/4}|B|^{1/2}|L|^{3/4} = p^{11/4}$. Note that for $\mathbb{F}_q$ with $q = p^r$, the condition remains $|A||L| \leq p^2$, so in this case the theorem applies only to very small sets, specifically with $|A||L| \leq |\mathbb{F}|^{2/r}$. Over a field of characteristic zero, like $\mathbb{C}$, the condition $|A||L| \leq p^2$ can be omitted (thanks to the convention that $p = \infty$).

The bound is tight in certain cases by the construction that we gave after Theorem 2.1. Indeed, there we had $|P| = |A||B|$, $|L| = |B|^2/|A|$, and $|I(P, L)| \gg |B|^2$, while Theorem 3.8 gives $|I(P, L)| \ll |A|^{3/4}|B|^{1/2}(|B|^2/|A|)^{3/4} = |B|^2$. However, when $|L|$ is away from the lower bound $|B|^2/|A|$, the bound in Theorem 2.1 is considerably stronger.

We now start our sketch of the proof, which consists of three steps: We convert point-line incidences in $\mathbb{F}^2$ to point-plane incidences in $\mathbb{F}^3$, which we convert to line-line intersection points in $\mathbb{F}^3$, and then we prove a bound on such intersection points.

From point-line incidences to point-plane incidences. We begin our sketch of the proof of Theorem 3.8. Define the "dual" of the line set L by

$$L^* = \{(s, t) \in \mathbb{F}^2 : y = sx + t\}.$$

This set does not account for any vertical lines that may be in L, but they altogether give at most $|A||B|$ incidences (since there are at most $|A|$ vertical lines that contain a point of $A \times B$, and each contains at most $|B|$ points), and using the condition $|B|^2/|A| \leq |L|$ we can check that $|A||B| \leq |A|^{3/4}|B|^{1/2}|L|^{3/4}$. Thus we can assume that $|L^*| = |L|$. Using the

Cauchy-Schwartz inequality we have

$$\begin{aligned}|I(A\times B,L)| &= |\{(x,y,s,t)\in A\times B\times L^* : y = sx+t\}|\\ &= \sum_{b\in B}|\{(x,s,t)\in A\times L^* : b = xs+t\}|\\ &\le |B|^{1/2}\left(\sum_{b\in B}|\{(x,s,t)\in A\times L^* : b = xs+t\}|^2\right)^{1/2}\\ &\le |B|^{1/2}|\{(x,s,t,x',s',t')\in (A\times L^*)^2 : xs+t = x's'+t'\}|^{1/2}.\end{aligned}$$

The set $\{(x,s,t,x',s',t')\in (A\times L^*)^2 : xs+t = x's'+t'\}$ can be interpreted as a set of incidences between points (x,s',t') and planes $sX+t = x'Y+Z$. Note that we split the variables in this particular way to make the resulting equations linear, and that this split happens to be possible because of the Cartesian product structure of the point set.

Define a point set and a plane set by

$$R = A\times L^*,\quad S = \{sX+t = x'Y+Z : (x',s,t)\in A\times L^*\}.$$

Then we have (with $I(R,S)$ denoting the set of point-plane incidences)

$$|I(P,L)|\le |B|^{1/2}|I(R,S)|^{1/2}.$$

Now we use the following point-plane incidence bound of Rudnev [19].

Theorem 3.9. *Let $R\subset\mathbb{F}^3$ and let S be a set of planes in $\mathbb{F}^3$. Assume that $|R|\le|S|$, that $|R|\le p^2$, and that R has no k points collinear. Then*

$$|I(R,S)|\ll |R|^{1/2}|S| + k|S|.$$

Applying this bound with $k = |A|^{1/2}|L|^{1/2}$ would give

$$|I(P,L)|\le |B|^{1/2}\left(|A|^{3/2}|L|^{3/2}\right)^{1/2} = |A|^{3/4}|B|^{1/2}|L|^{3/4},$$

the bound in Theorem 3.8. But we have to verify the conditions. We have $|R| = |S|$ and we assumed $p^2\ge |A||L| = |R|$. The condition that R has no $k = |A|^{1/2}|L|^{1/2}$ points collinear actually need not hold, but we can modify L to make it hold.

Because of the product structure of $R = A\times L^*$, the maximum number of collinear points in R equals the maximum of $|A|$ and the maximum number of concurrent lines in L. Indeed, $A\times L^*$ is covered by $|L^*|$ lines parallel to the x-axis, each containing $|A|$ points. Another line either equals one of these parallel lines and thus contains $|A|$ points, or it intersects each of the parallel lines in at most one point. In the latter case, we can project to the yz-plane to see that the number of points of $A\times L^*$ on the line is at most the number of points of L^* on its projection. By duality, the maximum number of collinear points in L^* equals the maximum number of concurrent (or parallel) lines in L.

We clearly have $|A|\le |A|^{1/2}|L|^{1/2}$, which is the bound we want, but L could have more than $|A|^{1/2}|L|^{1/2}$ concurrent lines. To avoid this, we can modify L beforehand by removing every pencil of at least $|A|^{1/2}|L|^{1/2}$ concurrent (or parallel) lines. We do this by iteratively removing the largest pencil L_i, in at most $|L|/(|A|^{1/2}|L|^{1/2})$ steps. Such a pencil has $|L_i|$ incidences at its concurrency point, and at most $|A||B|$ other incidences. Thus in total we remove at most

$$\frac{|L|}{|A|^{1/2}|L|^{1/2}}\cdot|A||B| + \sum|L_i|\le |A|^{1/2}|B||L|^{1/2} + |L|\le |A|^{3/4}|B|^{1/2}|L|^{3/4}$$

incidences, where we used $|B|^2/|A| \leq |L|$ to get $|A|^{1/2}|B||L|^{1/2} \leq |A|^{3/4}|B|^{1/2}|L|^{3/4}$, and we used $|L| \leq |A||B|^2$ to get $|L| \leq |A|^{3/4}|B|^{1/2}|L|^{3/4}$.

To summarize, after preparing L by removing pencils, we obtain a point set R with no $|A|^{1/2}|L|^{1/2}$ points collinear, so that Theorem 3.9 gives the bound in Theorem 3.8.

From point-plane incidences to line-line intersections. We now proceed to prove Theorem 3.9. Note that the bound is tight for $k \geq |R|^{1/2}$, because if we take R to be k points on some line, and we let S consist of planes containing that line, then we get $|I(R,S)| = k|S|$. By a more sophisticated construction [19], the bound is still tight for smaller k and $\mathbb{F} = \mathbb{F}_p$ with $|R|$ close to p^2. We take a smooth cubic surface in $\mathbb{F}_p^3$, which has p^2 points. A standard result in algebraic geometry is that such a surface contains at most 27 lines, so we can remove the points on these lines and still have $\Omega(p^2)$ points (for p sufficiently large), but no four collinear by Bézout's inequality. Most planes will contain $\Omega(p)$ of these points, so for most plane sets S we get $\Omega(p|S|) = \Omega(|R|^{1/2}|S|)$ incidences.

We define a parameter space for the set of lines in $\mathbb{F}^3$ that pass through a fixed line. For concreteness, define a line λ and a plane π by

$$\lambda = \{(0,0,z) : z \in \mathbb{F}\}, \quad \pi = \{(1,y,z) : y,z \in \mathbb{F}\}.$$

We parametrize the set of lines that pass through λ (as well as π) by the following rule:

If a line ℓ hits λ in $(0,0,a)$ and π in $(1,b,c)$, then $\ell^* = (a,b,c)$.

This gives a correspondence between points in $\mathbb{F}^3$ and lines ℓ in $\mathbb{F}^3$ that hit λ and π.

We use this parametrization to map points and planes to lines and lines. For a point r in $\mathbb{F}^3$ that is not on the yz-plane, we define

$$\varphi(r) = \{\ell^* : \ \ell \text{ hits } r \text{ and } \lambda\ \},$$

and for a plane s in $\mathbb{F}^3$ that hits λ in exactly one point, we define

$$\psi(s) = \{\ell^* : \ \ell \text{ lies in } s \text{ and hits } \lambda\ \},$$

The sets $\varphi(r)$ and $\psi(s)$ are both lines, which is easy to check via the parametrization. Moreover, we have an incidence $r \in s$ if and only if the lines $\varphi(r)$ and $\psi(s)$ intersect.

We can apply a generic linear transformation to $\mathbb{F}^3$ so that none of the points in R lies on the yz-plane, and so that each plane in S hits λ in exactly one point. Then we have

$$|I(R,S)| = |I(\varphi(R), \psi(S))|,$$

where for two line sets L, M we write $I(L,M)$ for the set of points where a line of L intersects a line of M. Now we apply the following bound on intersection points of Guth and Katz [7].

Theorem 3.10. *Let L and M be sets of lines in $\mathbb{F}^3$. Assume that $|L| \leq |M|$, that $|L| \leq p^2$, and that no quadric contains k lines of L and k lines of M in different rulings. Then*

$$|I(L,M)| \ll |L|^{1/2}|M| + k|M|.$$

This clearly gives the bound in Theorem 3.9, if we can show that the conditions hold. Clearly $|\varphi(R)| = |\psi(S)|$ and $|\varphi(R)| \leq p^2$ by assumption. For the third condition, we need some context. A *quadric* or *quadric surface* is a solution set in $\mathbb{F}^3$ of a quadratic polynomial from $\mathbb{F}[x,y,z]$. If a smooth quadric contains a line, then it contains two infinite

families of lines, called *rulings*. For example, the quadric $z = xy$ contains lines of the form $\{(s, y_0, sy_0) : s \in \mathbb{F}\}$ and lines of the form $\{(x_0, t, x_0 t) : t \in \mathbb{F}\}$. Two lines on a smooth quadric intersect if and only if they are in opposite rulings. A singular quadric can be a double plane or a cone; a plane has infinitely many rulings (a pencil of lines through each point) and a cone has only one ruling. Note that if $\mathbb{F}$ is not algebraically closed, then some quadrics may contain no lines, like a sphere in $\mathbb{R}^3$, but this is no problem for us.

To finish deducing Theorem 3.9 from Theorem 3.10, suppose that a quadric Q contains k lines of $\varphi(R)$ and k lines of $\psi(S)$ in different rulings. We assume that we have applied a generic transformation to R and S, which implies that no two lines in $\varphi(R)$ intersect (otherwise they would lie in the same plane containing λ, which the generic transformation can avoid). Because Q contains at least three disjoint lines, it must be a smooth quadric (because in a double plane or a cone, at least two out of every three lines intersect). Since the lines are in different rulings, each of the k lines from $\varphi(R)$ intersects each of the k lines from $\psi(S)$. This means that each of the corresponding k points of R are incident to each of the corresponding k planes of S. But, since we can assume $k \geq 3$, this is only possible if the k points are collinear, which contradicts the assumption of Theorem 3.9.

Proving the line-line intersection bound. We now sketch the proof of Theorem 3.10, up to some technical results from algebraic geometry. Given our two line sets L and M in $\mathbb{F}^3$, we use interpolation to find a surface Z containing all the lines in L, which we can do with $\deg(Z) \ll |L|^{1/2}$. We split Z into irreducible components as $Z = Z_1 \cup \cdots \cup Z_m$, with each Z_i irreducible and $\sum \deg(Z_i) \ll |L|^{1/2}$.

First we bound the number of intersection points between a line that is contained in some Z_i and a line that is not contained in that Z_i. Any line has at most $\deg(Z)$ intersection points with components that do not contain it, which gives a total of $(|L| + |M|)\deg(Z) \ll |L|^{1/2}|M|$ intersection points of this type. After this, it suffices to assign each line of L or M to one component containing it (say the one with smallest index), and to bound the intersection points between lines assigned to the same component. Let L_i and M_i be the sets of lines assigned to Z_i.

Suppose that Z_i is a plane or a smooth quadric. By assumption Z_i contains at most k lines of L, which lead to at most $k|M_i|$ incidences in Z_i, and a total of $\sum k|M_i| \leq k|M|$ incidences.

Suppose that Z_i is not a plane or smooth quadric. In this case we require more algebraic geometry. By work of Guth and Zahl [8], there exists a surface X_i of degree $\deg(X_i) \ll \deg(Z_i)$, such that for most $p \in Z_i$ we have $p \in X_i$ if and only if there are two lines through p contained in Z_i. Moreover, because Z_i is not a plane or smooth quadric, we have $\dim(X_i \cap Z_i) \leq 1$. Every intersection point of L_i and M_i is contained in X_i. If a line of L_i has at most $\deg(X_i)$ intersection points in Z_i, then we can bound these as above, while if a line has more intersection points, then it is contained in $X_i \cap Z_i$. By a technical lemma from algebraic geometry (see [12, Proposition 14]), the curve $X_i \cap Z_i$ has at most $\deg(X_i)\deg(Z_i)(\deg(X_i) + \deg(Z_i)) \ll \deg(Z_i)^{3/2}$ singular points, which include the intersection points of lines contained in $X_i \cap Z_i$. In total we get $\sum O(\deg(Z_i)^{3/2}) \ll |L|^{1/2}|M|$ intersection points in this way. This concludes the proof of Theorem 3.10.

3.4 Sum-product bounds over arbitrary fields

As in the last section, we let $\mathbb{F}$ be an arbitrary field of characteristic p, with $p = \infty$ in characteristic zero. We give analogues of the corollaries in Section 2.2. The first two corollaries were first derived from Rudnev's Theorem 3.9 directly, by Roche-Newton, Rudnev, and Shkredov [15], while the third was first observed by Stevens and De Zeeuw [24].

Corollary 3.11 (Roche-Newton–Rudnev–Shkredov). *If $A \subset \mathbb{F}$ satisfies $|A| \leq p^{5/8}$, then*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{6/5}.$$

Proof. Define

$$P = (A+A) \times (A \cdot A), \quad L = \{y = b(x-a) : a, b \in A\}.$$

Let M be the smaller one of $|A+A|, |A \cdot A|$ and let N be the larger one. We can assume that $M \leq |A|^{6/5}$, so that the condition $M|L| \leq p^2$ of Theorem 3.8 follows from $|A| \leq p^{5/8}$. The other condition of Theorem 3.8 is $N^2/M \leq |L| \leq M^3N^2$; the upper bound on $|L|$ is obvious, and if the lower bound failed we would have $|A|^2 < N^2/M$, which would give $N > |A|\sqrt{M} \geq |A|^{3/2}$. Therefore, we can apply Theorem 3.8 to get

$$|A|^3 \leq I(P, L) \ll M^{3/4}N^{1/2}|A|^{3/2},$$

which gives $M^3N^2 \gg |A|^6$ and proves the corollary. □

Corollary 3.12 (Roche-Newton–Rudnev–Shkredov). *If $A \subset \mathbb{F}$ satisfies $|A| \ll p^{2/3}$, then*

$$|A + A \cdot A| \gg |A|^{3/2}.$$

Proof. Define

$$P = A \times (A + A \cdot A), \quad L = \{y = a + bx : a, b \in A\}.$$

The condition $|A||L| \leq p^2$ of Theorem 3.8 corresponds to $|A| \leq p^{2/3}$. The condition $|L| \leq |A|^3|A + A \cdot A|^2$ is obvious, and if the condition $|A + A \cdot A|^2/|A| \leq |L| = |A|^2$ fails, then we are done. Thus we get

$$|A|^3 = |I(P, L)| \ll |A|^{3/4}|A + A \cdot A|^{1/2}|A|^{3/2},$$

and we are done. □

Corollary 3.13 (Stevens–De Zeeuw). *Let $f(x, y) = x^2 + xy$. If $A \subset \mathbb{F}$ satisfies $|A| \ll p^{2/3}$, then*

$$|f(A, A)| \gg |A|^{5/4}.$$

Proof. We define

$$P = A \times A, \quad L = \{f(s, x) = f(t, y) : s, t \in A\}.$$

The conditions of Theorem 3.8 are easy to check, so we get

$$\frac{|A|^4}{|f(A, A)|} \ll |I(P, L)| \ll |A|^{3/4}|A|^{1/2}(|A|^2)^{3/4} = |A|^{11/4}$$

and we are done. □

Bibliography

[1] Noga Alon and Joel Spencer, *The probabilistic method*, third edition, John Wiley & Sons, Hoboken, 2008.

[2] Boaz Barak, Russell Impagliazzo, and Avi Wigderson, *Extracting randomness using few independent sources*, SIAM Journal on Computing **36**, 1095–1118, 2006.

[3] György Elekes, *On the number of sums and products*, Acta Arithmetica **81**, 365–367, 1997.

[4] György Elekes, Melvyn Nathanson, and Imre Ruzsa, *Convexity and sumsets*, Journal of Number Theory **83**, 194–201, 1999.

[5] Paul Erdős and Endre Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics (To the memory of Paul Turán), Birkhäuser Verlag, 213–218, 1983.

[6] Moubariz Garaev, *The sum-product estimate for large subsets of prime fields*, Proceedings of the American Mathematical Society **136**, 2735–2739, 2008.

[7] Larry Guth and Nets Hawk Katz, *On the Erdős distinct distances problem in the plane*, Annals of Mathematics **181**, 1–36, 2015.

[8] Larry Guth and Joshua Zahl, *Algebraic curves, rich points, and doubly-ruled surfaces*, `arXiv:1503.02173`, 2015.

[9] Norbert Hegyvári, *On consecutive sums in sequences*, Acta Mathematica Hungarica **48**, 193–200, 1986.

[10] N. Hegyvári and F. Hennecart, *Conditional expanding bounds for two-variable functions over prime fields*, European Journal of Combinatorics **34**, 1365–1382, 2013.

[11] Do Duy Hieu and Le Anh Vinh, *On distance sets and product sets in vector spaces over finite rings*, Michigan Mathematical Journal **62**, 779–792, 2013.

[12] János Kollár, *Szemerédi–Trotter-type theorems in dimension* 3, Advances in Mathematics **271**, 30–61, 2015.

[13] Brendan Murphy and Giorgis Petridis, *A point-line incidence identity in finite fields, and applications*, Moscow Journal of Combinatorics and Number Theory **6**, 64–95, 2016.

[14] Liangpan Li and Jian Shen, *A sum-division estimate of reals*, Proceedings of the American Mathematical Society **138**, 101–104, 2010.

[15] Orit Raz, Micha Sharir, and József Solymosi, *Polynomials vanishing on grids: The Elekes-Rónyai problem revisited*, American Journal of Mathematics **138**, 1029–1065, 2016.

[16] Oliver Roche-Newton, *A short proof of a near-optimal cardinality estimate for the product of a sum set*, Proceedings of the 31st Symposium on Computational Geometry, 74–80, 2015.

[17] Oliver Roche-Newton and Misha Rudnev, *On the Minkowski distances and products of sum sets*, Israel Journal of Mathematics **209**, 507–526, 2015.

[18] Oliver Roche-Newton, Misha Rudnev, and Ilya Shkredov, *New sum-product type estimates over finite fields*, Advances in Mathematics **293**, 589–605, 2016.

[19] Misha Rudnev, *On the number of incidences between points and planes in three dimensions*, `arXiv:1407:0426`, 2014.

[20] Tomasz Schoen and Ilya Shkredov, *On sumsets of convex sets*, Combinatorics, Probability and Computing **20**, 793–798, 2011.

[21] George Shakan, post on the website *mathoverflow*, `https://mathoverflow.net/questions/168844/sum-and-product-estimate-over-integers-rationals-and-reals`, 2014.

[22] Micha Sharir, Adam Sheffer, and József Solymosi, *Distinct distances on two lines*, Journal of Combinatorial Theory, Series A **120**, 1732–1736, 2013.

[23] József Solymosi, *On distinct consecutive differences*, `arXiv:math/0503069`, 2005.

[24] Sophie Stevens and Frank de Zeeuw, *An improved point-line incidence bound over arbitrary fields*, `arXiv:1609:06284`, 2016.

[25] József Solymosi, *Incidences and the spectra of graphs*, Building Bridges, Bolyai Society Mathematical Studies **19**, 499–513, Springer, 2008.

[26] József Solymosi, *Bounding multiplicative energy by the sumset*, Advances in Mathematics **222**, 402–408, 2009.

[27] Endre Szemerédi and William T. Trotter, *Extremal problems in discrete geometry*, Combinatorica **3**, 381–392, 1983.

[28] Terence Tao and Van Vu, *Additive Combinatorics*, Cambridge University Press, Cambridge, 2006.

[29] Le Anh Vinh, *The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields*, European Journal of Combinatorics **32**, 1177-1181, 2011.