3 Sums and Products and More

In this section we will prove two lovely theorems in additive combinatorics which involve a little more than just sumsets. The first concerns a set of real numbers with both a small sumset and a small product set. The second concerns a subset of a finite vector space which contains an affine line in every direction.

Small Sumset and Product Set

For a set $A \subseteq \mathbb{R}$ we have already defined the sumset $A + A = \{a + a' \mid a, a' \in A\}$ and we also have the product set $A \cdot A = \{a \cdot a' \mid a, a' \in A\}$. We know that arithmetic progressions give very small sumsets and similarly geometric progressions will yield very small product sets. The following famous conjecture of Erdös and Szemerédi asserts that no large subset of real numbers can have both $A + A$ and $A \cdot A$ very small.

Conjecture 3.1 (Erdös-Szemerédi) *For every $\epsilon > 0$, every sufficiently large set $A \subseteq \mathbb{R}$ satisfies*

$$\max\{|A + A|, |A \cdot A|\} \geq |A|^{2-\epsilon}.$$

Our goal in this section will be to prove the following partial result toward this famous conjecture.

Theorem 3.2 (Elekes) *Let A be a finite subset of $\mathbb{R}$. Then $|A + A| \cdot |A \cdot A| \geq \frac{1}{64}|A|^{\frac{5}{2}}$.*

This theorem proves that every $A \subseteq \mathbb{R}$ must satisfy $\max\{|A + A|, |A \cdot A|\} \geq \frac{1}{8}|A|^{\frac{5}{4}}$ so it implies that Conjecture 3.1 holds true whenever ϵ is greater than $\frac{3}{4}$. The best known result (due to Solymosi) asserts that the conjecture holds true for any value of ϵ greater than $\frac{2}{3}$.

The line toward Theorem 3.2 is anything but straightforward, we will first take a detour into graph drawing and then to combinatorial geometry!

Crossing Number

We will assume that all graphs here are simple, that is, without loops or parallel edges. The *crossing number* of a graph G, denoted $cr(G)$, is the minimum number of pairwise crossings over all possible drawings of G in the plane. Note that any drawing achieving this minimum

will have the property that two adjacent edges do not cross (otherwise we may reroute and decrease the number of crossings).

Observation 3.3 *Every graph $G = (V, E)$ satisfies $cr(G) \geq |E| - 3|V|$.*

Proof: Suppose that G has crossing number c and consider a drawing of it with exactly c crossings. Modify G to form the graph $G' = (E', V)$ by the following process. For every pair of edges e, f which cross in the drawing, delete one of e, f. The resulting drawing of G' is a planar graph, so by Euler's Formula we must have $|E'| \leq 3|V|$. In total, this gives us $cr(G) = c \geq |E| - |E'| \geq |E| - 3|V|$ as desired. $\square$

Theorem 3.4 (Crossing Lemma) *If $G = (V, E)$ satisfies $|E| \geq 4|V|$ then*

$$cr(G) \geq \frac{|E|^3}{64|V|^2}.$$

Proof: Let $v = |V|$ and $e = |E|$ and $c = cr(G)$, and consider a drawing of G in the plane with exactly c crossings. Define $p = \frac{4v}{e} \leq 1$ and choose a random subset $V' \subseteq V$ by selecting each element independently with probability p. Let $E' = \{uv \in E \mid u, v \in V'\}$ and consider the graph G'. The drawing of G gives us a drawing of G', and assume this drawing has c' crossings. By the above observation we must have $0 \leq c' - e' + 3v'$. So, viewing c', e', v' as random variables we have

$$\begin{aligned} 0 &\leq \mathbb{E}[c'] - \mathbb{E}[e'] + 3\mathbb{E}[v'] \\ &= p^4 c - p^2 e + 3pv \\ &= p^4 \left(c - \frac{e^3}{16v^2} + \frac{3ve^3}{64v^3} \right) \\ &= p^4 \left(c - \frac{e^3}{64v^2} \right) \qquad \square \end{aligned}$$

Theorem 3.5 (Szemerédi, Trotter) *Let V be a set of points and L a set of lines in $\mathbb{R}^2$ and define $q = \#\{(p, \ell) \in P \times L \mid p \sim \ell\}$. Then we have*

$$q \leq 4\left(|V|^{2/3}|L|^{2/3} + |V| + |L|\right).$$

Proof: We may assume without loss that every line contains at least one point, since removing a pointless line would only improve the bound. Now we will construct a graph G

drawn in the plane from our points and lines as follows. We take V as the vertex set, and for any two consecutive points say p_1, p_2 on a line ℓ we add the edge p_1p_2 drawn as a straight line segment contained in ℓ. Now the edge set E of our graph will satisfy $|E| = \sum_{\ell \in L} (\#\{p \in V \mid p \sim \ell\} - 1) = q - |L|$. If $4|V| \geq |E| = q - |L|$ then we are done, so we may assume $|E| \geq 4|V|$. Observe that the drawing we have constructed of G has at most $|L|^2$ crossings since any two lines in L can meet at most once. So, the Crossing Lemma yields $|L|^2 \geq \frac{(q-|L|)^3}{64|V|^2}$ which completes the proof. $\square$

Proof of Theorem 3.2: Let $V = (A + A) \times (A \cdot A) \subseteq \mathbb{R}^2$ and note that $|A|^2 \leq |V| \leq |A|^4$. For every $a, b \in A$ let $\ell_{a,b}$ be the line in $\mathbb{R}^2$ given by the equation $y = a(x - b)$. and let $L = \{\ell_{a,b} : a, b \in A\}$. If $\ell_{a,b} \in L$, then for every $c \in A$ the line L is incident with the point $(b+c, a \cdot c) \in V$, so L is incident with $\geq |A|$ points. Thus, by the Szemerédi Trotter theorem we have

$$\begin{aligned} |A|^3 &= |A| \cdot |L| \\ &\leq 4\left(|A|^{\frac{4}{3}}|V|^{\frac{2}{3}} + |V| + |A|^2\right) \\ &\leq 16|A|^{\frac{4}{3}}|V|^{\frac{2}{3}}. \end{aligned}$$

Rearranging we get $\frac{1}{64}|A|^{\frac{5}{2}} \leq |V|$ which completes the proof. $\square$

The Kakeya Problem for Finite Fields

An old theorem due to Besicovich asserts that for every $\epsilon > 0$, there exists a set $B \subseteq \mathbb{R}^2$ with area at most ϵ so that B contains a unit line segment which can be turned around by moving it continuously within B. Although Besicovich's sets have small area, they are complex in the sense that they have Hausdorf dimension close to 2. The famous Kakeya conjecture asserts that in general, any subset of $\mathbb{R}^d$ which contains a line segment in every direction must have Hausdorf dimension close to d. There is a well-known analogous conjecture for finite fields which was recently solved by Dvir by way of the following result. Our goal here will be to give a proof of this nice combinatorial theorem.

Theorem 3.6 (Dvir) *Let $A \subseteq \mathbb{F}_q^n$ and assume that A contains an affine line in every direction. Then*

$$|A| \geq \binom{q+n-1}{n}.$$

Our proof will involve some basic properties of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$. Consider the polynomials which are expressed as a sum of monomials with no term raised to a power which is q or larger. That, is those polynomials of the form:

$$p(x_1, \ldots, x_n) = \sum_{0 \leq d_1 \ldots, d_n < q} c_{d_1, \ldots, d_n} x_1^{d_1} \ldots x_n^{d_n}$$

There are exactly q^{q^n} such polynomials, and they give rise to every possible function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. Therefore, the only such polynomial which identically evaluates to zero is the zero polynomial. It follows from this that anytime we have a polynomial expression of degree $< q$ which is nontrivial, it must evaluate to a nonzero value on some input.

Lemma 3.7 *Let* $\mathbf{a_1}, \ldots, \mathbf{a_m} \in \mathbb{F}_q^n$ *and assume* $m < \binom{n+d}{n}$. *Then there exists a nonzero polynomial* $p(x_1, \ldots, x_n)$ *of degree at most* d *for which* $p(\mathbf{a}_i) = 0$ *for every* $1 \leq i \leq m$.

Proof: Consider a general polynomial of degree at most d in these coefficients

$$p(x_1, \ldots, x_n) = \sum_{d_1 + \ldots + d_n \leq d} c_{d_1, \ldots, d_n} x_1^{d_1} \ldots x_n^{d_n}.$$

Now consider these coefficients $c_{d_1 \ldots, d_n}$ as variables and note that we have exactly $\binom{n+d}{n}$ of these coefficients. The constraint that $p(\mathbf{a}_i) = 0$ gives us a homogeneous linear equation which must be satisfied by our coefficients. Since we have more variables than constraints, there exists a nontrivial solution. That is, there exists a nontrivial polynomial of degree at most d which vanishes on every $\mathbf{a}_i$. $\square$

Proof of Theorem 3.6: By the previous lemma, we may choose a nontrivial polynomial p of degree $d < q$ which vanishes on every point in A. Now let $\mathbf{b} \in \mathbb{F}_q$ and choose $\mathbf{a} \in A$ so that $\mathbf{a} + t\mathbf{b} \in A$ for every $t \in \mathbb{F}_q$. Consider the polynomial given by $f(t) = p(\mathbf{a} + t\mathbf{b})$. Since p is zero on every point of A we see that the polynomial $f(t)$ must evaluate to 0 on every input. We can express $f(t)$ as the following polynomial of degree d

$$f(t) = p(\mathbf{a} + t\mathbf{b}) = \sum_{d_1 + \ldots + d_n \leq d} c_{d_1 \ldots d_n} (a_1 + tb_1)^{d_1} \ldots (a_n + tb_n)^{d_n} \tag{1}$$

Now, the expression on the right hand side has degree at most $d < q$. This together with the fact that $f(t) = 0$ implies that the coefficient of t^d on the right hand side must be 0. Define the polynomial $\overline{p}$ to be given by taking all monomials of p with degree exactly d. We see that

the coefficient of t^d in the expansion of the right hand side of 1 is exactly $\overline{p}(\mathbf{b})$. This gives us $\overline{p}(\mathbf{b}) = 0$, and this must hold for every $\mathbf{b} \in \mathbb{F}_q$. However, this contradicts the assumption that $\overline{p}$ is nontrivial. $\square$