Algebraic Methods Notes

Kenneth Moore
University of British Columbia

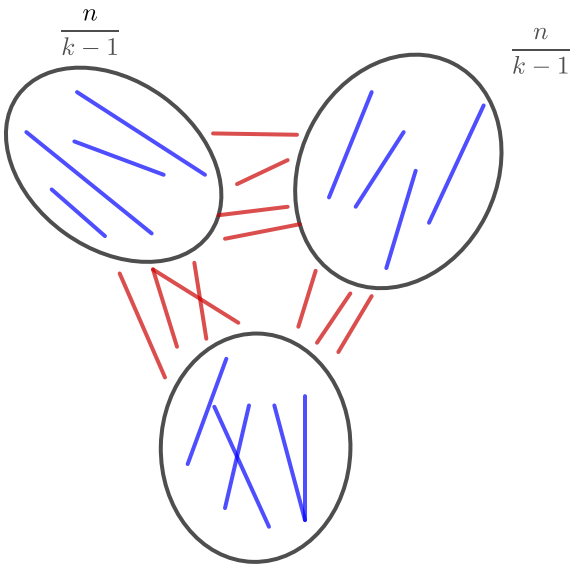
May 30 → June 2, 2023

Lecture 1 – *Explicit Constructions for Bipartite Turán Problems 1* – Tibor Szabó

Themes or the week: Bipartite Turán numbers, Pseudorandom graphs, the Szemeredi-Trotter theorem, Sum-product Estimates, Slice rank, and Kakeya. We begin, of course, with Ramsay.

Theorem 1.1 (Ramsay, E-Sz)**.** $R(k) \leq 4^k$.

This led to Turáns theorem – what if we just try to get as many red edges as possible without a red K_k and ignore what happens to the blue edges? Turan created the Turan graph. It has blue cliques which are joined by red edges in a bipartite fashion.



Theorem 1.2 (Turán)**.** $ex(n, K_k) = e(T_{n,k-1}) = \left(1 - \frac{1}{k-1}\right)\binom{n}{2} + O(n)$

This was conjectured to be the best graph in Ramsay's theorem, but Erds disproved this.

Theorem 1.3 (Erdős)**.** $R(k) \geq \sqrt{n}^k$.

Btw, the definition of the ex thing is

Definition 1.4 (Turán number)**.** *The Turán number or extremal number of H is*

$$ex(n, H) := \max\left(m \in \mathbb{N} : \exists H\text{-free graph } G,\ v(G) = n,\ e(G) = m\right) \tag{1.1}$$

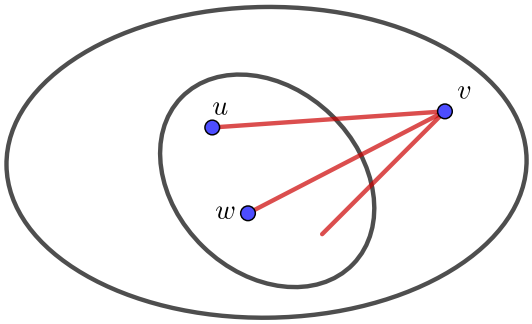
Turán had a question: what were the extremal numbers for the platonic solids? He conjectured that $ex(n, H) = \left(1 + \frac{1}{3}\right)\binom{n}{2} + O(n)$ was true. Today, all of these have been provan true except for the cube!

Theorem 1.5 (Erdős-Stone)**.** *For all H,*

$$ex(n, H) = \left(1 + \frac{1}{\chi(H) - 1}\right)\binom{n}{2} + O(n^2)\,. \tag{1.2}$$

This is an asymptotic answer for all graphs where $\chi(H) \geq 3$, but for less than 3 the second term dominates! That's why the cube is hard, since $\chi(H) = 2$.

Theorem 1.6 (Erdős, 1936)**.** $ex(n, K_{2,2}) \leq \frac{1}{2}n^{3/2}$



Proof. Graph G is $K_{2,2}$ free iff for all $u, v \in V$, there is at most 1 common neighbour. Therefore,

$$\binom{n}{2} > \sum_{u,w,\in V, w\neq w} d(u, w) = \#K_{1,2} \text{ in } G = \sum_{v\in V}\binom{d(v)}{2} \geq n \cdot \binom{\overline{d}(G)}{2}\,, \tag{1.3}$$

where the last inequality follows from Jensen's inequality, for $x \mapsto \binom{x}{2}$. (Notation, $\overline{d}(G)$ is the average degree of G.) Thus,

$$n - 1 \geq \overline{d}(G)\left(\overline{d}(G) - 1\right) \implies \overline{d}(G) \leq \sqrt{n}\,. \tag{1.4}$$

□

Erdős was very pleased with this proof, how can we get we some of that magic? If we try random constructions, (let $m = \binom{n}{2}$?) $G(m, p)$, a $K_{2,2}$ will appear when $p \approx \frac{1}{n}$. With this probability, the number of edges $e(G(n, p))$ is around $p\binom{n}{2} = \Theta(n)$. So this is not great.

What about this alteration,

$$\mathbb{E}\left(e(G(n, p)) - \#K_{2,2} \text{ in } G(m, \frac{1}{2})\right) \geq \frac{1}{2}p\binom{n}{2}\,. \tag{1.5}$$

(Note that the $\#K_{2,2}$ in $G(m, \frac{1}{2})$ should be around n^4p^4? Also, should that really be $G(m, \frac{1}{2})$?) Picking a probability $p = cn^{-2/3}$, this leads to a graph with about $cn^{4/3}$ edges. Now we are

considering an infinite graph, with the vertices being points and lines in $\mathbb{R}^2$, connected by an edge if the line goes through the point. This graph is $K_{2,2}$ free, with size...

$$|\mathbb{R}| + |\mathbb{R} \cup \{\infty\}| \, |\mathbb{R}| \approx 2 \, |\mathbb{R}|^2 \tag{1.6}$$

and degree around $|\mathbb{R}|^2$. The number edges is

$$e(G) = \left(\frac{1}{2} \cdot |\mathbb{R}|^2 \, |\mathbb{R}| \right) = \left(\frac{v(G)}{2} \right)^{3/2} . \tag{1.7}$$

This line of reasoning of course is kinda nonsensical, but we can instead do this over $\mathbb{F}_q$ and it will actually make sense. If you do this here, you will get $|V(G)| = q^2 + q^2 + q$ (the size of $\mathbb{F}_q$ plus the # of lines in $\mathbb{F}_q^2$). A line, btw, is what it should be, $\ell_{a_1,a_2,a_3} := \left\{ (x,y) \in \mathbb{F}_q^2 : a_1 x + a_2 y = a_3 \right\}$. Now we have $e(G) = (q^2+q) \cdot q \approx \left(\frac{n}{2}\right)^{3/2} = \frac{1}{2\sqrt{2}} n^{3/2}$.

Now we talk about the projective plane. The points are linear spaces in $\mathbb{F}^3$, lines are the 2-dim linear spaces in $\mathbb{F}^3$. Formally, a point in the projective plane is a triple $[(a_0, a_1, a_2)] = \left\{ \lambda(a_0, a_1, a_2) \neq \overrightarrow{0} : \lambda \in \mathbb{F}_q^* \right\}$, and a line is $L(a_0, a_1, a_2) = \{[x_0, x_1, x_2] : a_0 x_0 + a_1 x_1 + a_2 x_2 = 0\}$

Exercise 1.7. *There are $q^2 + q + 1$ points in $PG(2, g)$ and as many lines such that every line contains $q + 1$ points, every point has $q + 1$ lines passing through it, and every two lines intersect in exactly one point.*

The Eszter Klein Graph has $v(G) = 2(q^2 + q + 1)$ and $e(G) = (q^2 + q + 1)(q + 1) \approx \frac{1}{2\sqrt{2}} n^{3/2}$.

Exercise 1.8. *Prove the EK-graph is optimal for $q^2 + q + 1$ points and lines while being $K_{2,2}$ free.*

So then why are we missing the constant factor? In $\mathbb{F}_q$, we could instead create the Polarity graph. (Brown, Erdős-Rényi-Sós) Take the vertices to be the triples

$$P - \left\{ [a_0, a_1, a_2] : (a_0, a_1, a_2) \subset \mathbb{F}_q^3 \backslash \{(0,0,0)\} \right\} ,$$

and the edge set $\{[a][\ell] : a_0\ell_0 + a_1\ell_1 + a_2\ell_2 = 0\}$. Then The edge set has size $\frac{1}{2}(q^2 + a + 1)(q + 1) - q + 1 \approx \frac{1}{2} n^{3/2}$ (the subtracted bit is because of loops!). Finally,

Theorem 1.9 (Furedi)**.** $ex((q^2 + q + 1), K_{2,2}) = e(G)$

Theorem 1.10 (Kovári-Sós-Turán)**.** *for $t \leq s$, then $ex(n, K_{t,s}) \leq \frac{(s-1)^{1/t}}{2} n^{2-\frac{1}{t}} + O(n)$*

This gives us a lower bound of $\frac{1}{2} n^{3/2}$ on all $ex\,(n, K_{2,t})$ using the previous stuff. Furedi also showed that $ex\,(n, K_{2,t}) \leq \frac{\sqrt{s-1}}{2} n^{3/2}$. And at last,he also showed that $ex(n, K_{3,3}) = Cn^{2-\frac{1}{3}}$.

Lecture 2 – *Explicit Constructions for Bipartite Turán Problems 2* – Tibor Szabó

Can we use incidence geometry for more things? For a $K_{3,3}$ free graph, we need that for all triples $a, b, c \in V(G)$ of vertices, the neighbourhoods $|N(a) \cap N(b) \cap N(c)| \leq 2$. Do a similar thing, let $V(G) = \mathbb{R}^3$ and $E(G) = \{x, y : (x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_2 - y_2)^2 = 1\}$. You can see that this infinite graph is $K_{3,3}$ free. Now, $degree(v) = |\mathbb{R}^2 \cup \{\infty\}| \approx |\mathbb{R}|^2$ and $e(G) \approx \frac{1}{2} |\mathbb{R}|^2 \, |\mathbb{R}|^3 \approx$

$\frac{1}{2}(v(G))^{5/3}$ which is the "right number", so this gives us the courage to try to make sense of this with $\mathbb{F}_p$ again.

[Brown, 1966] Suppose $|N(a) \cap N(b) \cap N(c)| \geq 3$. Let x be in $N(b) \cap N(c)$. Then we can find

$$\begin{aligned}(x_1 - a_1)^2 + (x_2 - a_2)^2 + (x_3 - a_3)^2 &= \alpha \\ (x_1 - b_1)^2 + (x_2 - b_2)^2 + (x_3 - b_3)^2 &= \alpha \\ (x_1 - c_1)^2 + (x_2 - c_2)^2 + (x_3 - c_3)^2 &= \alpha\end{aligned}$$

we can subtract these equations and move this to matrix form, to obtain

$$\begin{bmatrix} a_1 - b_1 & a_2 - b_2 & a_3 - b_3 \\ b_1 - c_1 & b_2 - c_2 & b_3 - c_3 \\ c_1 - a_1 & c_2 - a_2 & c_3 - a_3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 0 \tag{2.1}$$

If rank is 2, there are 3 solutions on one line. If the rank is 1m then a, b, c are on a line. Both of these would (intuitively?) imply that there is $K_{3,3}$ in your graph.

If $\ell \subseteq N(a)$, then we should shift everything so that ℓ goes through the origin. Let $\ell = \{\tau v : \tau \in \mathbb{F}_p\}$ for a $v \in \mathbb{F}_p^3 \setminus \{0\}$. W.l.o.g. suppose $v_1 \neq 0$. Doing the translation, we know

$$(\tau v_1 - a_1)^2 + (\tau v_2 - a_2)^2 (\tau v_3 - a_3)^2 = \alpha \tag{2.2}$$

has at least 3 solutions in τ. Factoring, we have

$$\tau^2(v_1^2 + v_2^2 + v_3^2) - 2\tau(v_1 a_1 + v_2 a_2 + v_3 a_3) + a_1^2 + a_2^2 + a_3^2 = \alpha \tag{2.3}$$

which can only have $(v_1^2 + v_2^2 + v_3^2) = 0$, $(v_1 a_1 + v_2 a_2 + v_3 a_3) = 0$, and $a_1^2 + a_2^2 + a_3^2 = \alpha$ for this to have 3 solutions. Therefore

$$\alpha = a_1^2 + a_2^2 + a_3^2 = \left(\frac{-v_2 a_2 - v_3 a_3}{v_1}\right)^2 + \frac{a_2^2 + a_3^2}{v_1^2}(-v_2^2 - v_3^2) = -\frac{(v_2 a_3 + a_2 v_3)^2}{v_1^2}\,, \tag{2.4}$$

which is a contradiction if $-\alpha$ is not a square in $\mathbb{F}_p$ (for example, $\alpha = 1$, $p \equiv 3 \mod 4$). Now recall that $\left\{z \in \mathbb{F}_p^* : \exists x \in \mathbb{F}^p, x^2 = z\right\} = \frac{p-1}{2}$.

All this implies that the Brown graph is $K_{3,3}$ free. Take $\sum_{\alpha \in \mathbb{F}_p} \#\left\{a \in \mathbb{F}_p^3 : a_1^2 + a_2^2 + a_3^2 = \alpha\right\} = p^3$. The "average" then is $\frac{p^3}{p} = p^2$.

Exercise 2.1. *count the solutions to $x^2 + y^2 = \beta$ with $\beta \in \mathbb{F}_p$, and the sols to $x^2 + y^2 + z^2 = \beta$. The answer depends on quadratic residue-ness of β. (The potential answers are $p+1$, $p-1$, $2p-1$ and 1, the latter two coming from when β is a square?)*

In our case you'll find $p^2 - p$ such sols. Thus we have found a $K_{3,3}$-free graph with $\frac{1}{2}p^3(p^2 - p) \geq \frac{1}{2}n^{5/3}$ edges. Thus, the inequality stood at

$$\frac{1}{2}n^{5/3} \leq ex(n, K_{3,3}) \leq \frac{2^{1/3}}{2}n^{5/3}\,, \tag{2.5}$$

but Furedi showed that the lower bound is tight.

Now, we know the asymptotic for $ex(n, K_{2,s}) \approx \frac{\sqrt{s-1}}{2}n^{3/2}$, and $ex(n, K_{3,s}) \approx C_s n^{3/2}$ but the same is not true for $s > 3$. We do know that $ex(n, K_{4,4}) = O(n^{7/4})$. If we tried the randomness like we did before, we would get $n^{2-\frac{8-2}{16-1}} = n^{2-\frac{6}{15}} = n^{1.6}$, not so good.

It is an open problem to even show that $\frac{ex(n,K_{4,4})}{n^{5/3}} \to \infty$ or not. We might want to try the same thing over $\mathbb{F}_p^4$, with $\sum_{i=1}^4 (x_i - a + i)^2 = 1$, $xa \in E(G)$. It is an exercise to show that this contains a $K_{p,p} = K_{n^{1/4},n^{1/4}}$.

Another try, let's take $V = \mathbb{F}_p^4$, and $E = \left\{ab : \prod_{i=1}^4 (a_i + b_1) = 1\right\}$. This also fails! The problem with 4 is that it is 2+2. You can take elements like $(x, 1/x, 0, 0)$ and $(0, 0, z, 1/z)$ to get a huge bipartite graph, $(a_1 + b_1)(a_2 + b_2)(a_3 + b_3)(a_4 + b_4) = 1$.

One last try. This example was created by Kollár, Rónyai, Sz. Take $V(G) = \mathbb{F}_{q^t}$ for all prime power $t \in \mathbb{N}_+$, and $E(G) = \{AB : N(A + B) = 1\}$, where $N : \mathbb{F}_{q^t} \mapsto \mathbb{F}_q$, $N(X) := X^{\frac{q^t-1}{q-1}} = X \cdot X^q \cdot X^{q^2} \cdot X^{q^3}$. This 'norm' has the property that $N(X) \in \mathbb{F}_q$, $N(X)^{q-1} = X^{q^t-1} = 1$ (by Lagrange). Also, for all $\alpha \in \mathbb{F}_q^*$, $|N^{-1}(\alpha)| = \frac{q^t-1}{q-1}$. This all means that the 'normgraph' has the right number of edges. The degree of $A = \#\{X \in \mathbb{F}_{q^t} : N(X + A = 1\} = |N^{-1}(1)| - A = \frac{q^t-1}{q-1} \approx q^{t-1}$ as $t \mapsto \infty$ so that $e(G_{q,t)} \geq \frac{1}{2} q^t q^{t-1} = \frac{1}{2} n^{2-\frac{1}{t}}$

So how about the $K_{t,s}$-freeness of this? Well take $D_1, D_2, ..., D_t \in F_{q^t}$ distinct. We have $X \in \bigcap_{i=1}^t N(D_i)$, and

$$N(X + D_i) = 1 = (X + D_i) \cdot (X + D_1)^q \cdot (X + D_1)^{q^2} \cdot ... \cdot (X + D_1)^{q^{t-1}}$$
$$.....$$
$$N(X + D_t) = 1 = (X + D_i) \cdot (X + D_t)^q \cdot (X + D_t)^{q^2} \cdot ... \cdot (X + D_t)^{q^{t-1}}$$

because of characteristic, you can pull the powers inside, e.g. $(X + D_t)^{q^2} = (X^{q^2} + D_t^{q^2})$. We can use the following lemma to prove

Lemma 2.2 (Key lemma)**.** *If $\mathbb{F}$ is a field, and a_{ij}, $b_i \in \mathbb{F}$ with $a_{i_1,j} \neq a_{i_2 j}$ for all $i_1 \neq i_2$. Then the system of equations*

$$(x_1 - a_{11}) \cdot (x_2 - a_{12}) \cdot ... \cdot (x_t - a_{1t}) = b_1$$
$$... \qquad ...$$
$$(x_1 - a_{t1}) \cdot (x_2 - a_{t2}) \cdot ... \cdot (x_t - a_{tt}) = b_1$$

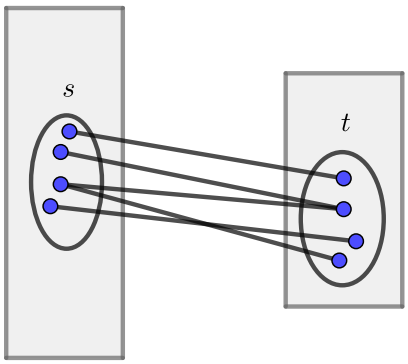
has at most $t!$ solutions.

So this construction works for $ex(n, K_{t,s})$ for all $s > t!$. We know $ex(n, K_{4,25}) = ex(n, K_{4,7}) = \Theta(n^{7/4})$, but $ex(n, K_{4,6})$ is unknown.

Lecture 3 – *Random Polynomials and Algebraic Geometry* – David Conlon

We will talk about the $z(m, n; s, t)$ problem – the maximum number of edges between a set U and V, with $|U| = m$, $|V|$ with no $K_{s,t}$ where the s vertices appear in U and the t vertices appear in V. Equivalently, this is the maximum nymber of 1s in a 0/1 matrix with no $s \times t$ all 1s submatrix.

In this context, the Kővári-Sós-Turán theorem says that $z(m, n; , s, t) \leq C(mn^{1-\frac{1}{s}} + n)$. Kollár-Rónyai-Szábo showed that $z(n, n; s, t) \geq cn^{2-\frac{1}{s}}$ provided that $t >> s$ (i.e. $t \geq s! + 1$). A.R.Sz. can improve this to $(s - 1)! + 1$.



Theorem 3.1. *For an $2 \le s \le t$ and $m \le n^{\frac{t^{\frac{1}{s}}}{s(s-1)}}$, we have $z(m,n;s,t) \ge c(mn^{1-\frac{1}{s}})$.*

This gets us K.R.Sz. back provided that $t \ge s^{2s} \implies t^{1/s} \ge s(s-1)$.

We will use the random algebraic method, and 'random' polynomials. See a paper by Matoušek, and one by Rödl-Sidorenko-Gunderson on these. There was a more powerful paper by Blagojevic-Bulth-Karasev; and one by Bulth. Then Bulth and the speaker did some good stuff.

We work over a finite field $\mathbb{F}_q$, where q is a prime power. We'll also need to talk about the algebraic closure of $\mathbb{F}_q$, which we write $\overline{\mathbb{F}}_q = \bigcup \mathbb{F}_{q^r}$.

Let $f(x)$ be a t-variable polynomial in variable $X = (X_1, \dots, X_t)$. The degree of f is the largest d s.t. there is a monomial $X_1^{a_1} X_1^{a_2} \dots X_t^{a_3}$ with $a_1 + \dots + a_t = d$. Eg, if $t = 2$ and $d = 3$, you could have $x^3, y^3, x^2y, xy^2, x^2, y^2, xy, x, y$. A random polynomial just has random coefficient from $\mathbb{F}_1$ on all monomials.

Lemma 3.2. *if $q > \binom{m}{2}$ and $d \ge m-1$, then the probability that $f(x_i) = 0$ for m points $x_1, \dots, x_m \in \overline{\mathbb{F}}_q^t$, where f is a t-variate degree d random polynomial is at most q^{-m}.*

Proof. suppose $x_i = (x_{i1}, x_{i2}, \dots, x_{it})$. Choose $a_2, \dots, a_t \in \mathbb{F}_q$ such that

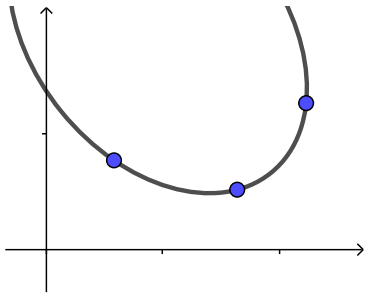
$$x_{i1} + \sum_{j=2}^{t} a_j x_{i,j} \neq x_{i'1} + \sum_{j=2}^{t} a_j x_{i',j} \tag{3.1}$$

for any $i \le i'$. The "negation" of this equation (replace the $\neq$ with $=$) has at most q^{t-2} solutions, so there are at most $\binom{m}{2}$ different equations and the number of $(a2, \dots, a_t)$ is q^{t-1}. So, since $q^{t-1} > \binom{m}{2} q^{t-2}$, there is a solution.

(Recall P_d is the set of random polynomials of degree at most d in $x_1, \dots, x_t$) Let $z_1 = x_1 + \sum_{j=2}^{t} a_j x_j$, and $z_j = x_j$. The set of polynomials P'_d in z are the same as P_d because change of variables is invertible. So, it suffices to show that a random $f \in P'_d$ goes through $z_1, \dots, z_m$ with probability q^{-m}. Note that $z_{i1} \neq z_{i'1}$ for all $i \neq i'$, which was the point of this change of variables.

Let p be a random polynomial in P'_d. We can write $p = g + h$, where h contains all monomials of the form z_1^j for $j = 0, \dots, m-1$, and g has every other monomial. For $p(z_i) = 0$, we need that actually $h(z_{i1}) = -g(z_{i1})$ (single variable thing... $h(z_i) = h(z_{i1})$). So we are just asking that a single variable function of degree $m-1$ passes through m given points.

We use Lagrange interpolation – there is exactly one polynomial of degree d which passes through any given $d+1$ points. Hence, there is exactly one choice of h with coefficients in $\overline{\mathbb{F}}_q$ with $h(z_{i1} = -g(z_i)$ for all i. If the polynomial is not over $\mathbb{F}_q$, there are no solutions. If it is in $\mathbb{F}_q$, there is exactly one solution out of a total of q^m.



□

The takeaway from this lemma is that degree d random polynomials are in some sense $d+1$-wise independent.

Definition 3.3. *A* variety *over an algebraically closed field $\overline{F}$ is a set of the form*

$$W = \left\{ x \in \overline{\mathbb{F}}^t : f_1(x) = ... = f_s(x) = 0 \right\} \tag{3.2}$$

for some polynomials $f_1, ..., f_s : \overline{\mathbb{F}}^t \mapsto \overline{\mathbb{F}}$. A variety is irreducible *if it cannot be written as the union of two proper subvarieties.*

Definition 3.4. *The dimension* $\dim(W)$ *of the variety W is the maximum d for which there is a chain of irreducible varieties $W_1, ..., W_d$, with*

$$\emptyset \subset \{p\} \subset W_1 \subset ... \subset W_d \subseteq W\,. \tag{3.3}$$

Over $\mathbb{F}_q$, there is a dichotomy whereby if you have dimension 0, then you have finitely many points (you can upper bound how many), and dimension ≥ 1 means you have at least $\frac{q}{2}$ points (this is just an approximation. The real number is more like $q - \sqrt{q}$).

Lemma 3.5 (Immediate from defn)**.** *If* $\dim(W) \geq 1$*, then W has infinitely many points over $\overline{\mathbb{F}}_q$.*

Lemma 3.6. *If $w \subseteq \overline{\mathbb{F}}^t$ is irreducible over $\overline{\mathbb{F}}$ and g is a hypersurface $\{g(x) = 0\}$ where $g : \overline{\mathbb{F}}^t \mapsto \overline{\mathbb{F}}$, then either $w \subseteq \{x : g(x) = 0\}$, or $w \cap \{x : g(x) = 0\}$ has dimension lower than w.*

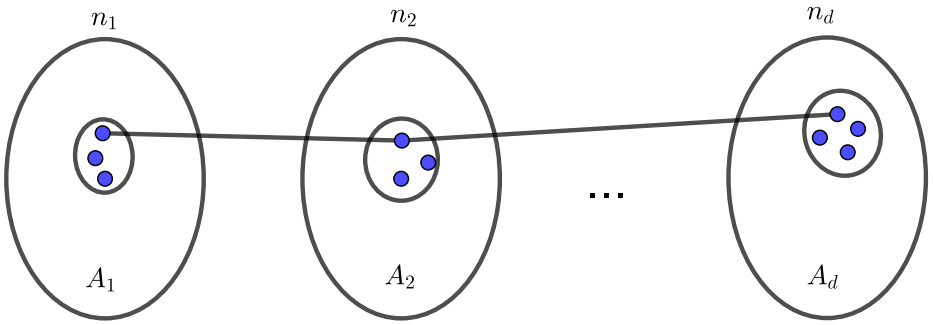
Theorem 3.7 (Bézout)**.** *If $f_1, ..., f_t : \overline{\mathbb{F}}^t \mapsto \overline{\mathbb{F}}$ and $W = \{x : f_1(x) = ... = f_t(x) = 0\}$ has* $\dim W = 0$*, then $|W| \leq d_1 d_2 ... d_t$ where $d_i = \deg f_i$.*

If $f_1, ..., f_s : \overline{\mathbb{F}}^t \mapsto \overline{\mathbb{F}}$ and $s < t$, then the number of irreducible components of the set $W = \{x : f_1(x) = ... = f_s(x) = 0\}$ is at most $d_1 d_2 ... d_s$.

So for example, if f_1 is a line, and f_2 has degree d, you can check using the fundamental theorem of algebra that there are at most d intersections unless there are all of them.

Lecture 4 – *Hypergraph Zarankiewicz 1* – Dmitrii Zakharov

A d-uniform hypergraph is a collection of d-element sets. We can take a fixed hypergraph H and consider $ex(n, H) = \max \#$ of edges on $[n]$ with no H. The problem now will be about the complete d-partite graph. How many edges can we add? so we consider $z(n_1, ..., n_d, s_i, ..., s_d) = \max |H|$ with no copy of $K^{(d)}_{s_1,...,s_d}$.



for $d = 2$ this is the same as $K_{2,2}$. The KST bound is that $ex(n, K_{s,t}) < n^{2-\frac{1}{t}}$. for an upper bound, we have

$$z(\overbrace{n...n}^{d}, \overbrace{2...2}^{d}) < n^{d-2^{-d+1}}, \tag{4.1}$$

H.W. is to prove this by induction.

Lower bounds are more interesting. Random: let $H \subset [n]^d$ each edge with probability p. Then $\mathbb{E}\,|H| = pn^d$ and $\mathbb{E}\#K^{(d)}_{2...2}$ in H =? Well if there are more than twice as many edges we can take an alteration to get a $K^{(d)}_{2...2}$ free K. We have $pn^d = p^{2^d}n^{2d}$ so we should choose $p = n^{-\frac{d}{2^d-1}}$. Thus the random construction gives us a lower bound of $\geq n^{d-\frac{d}{2^d-1}}$.

Another way, Algebraic: Let $d = 2$, take G on $(\mathbb{F}_p^2, \mathbb{F}_p^2)$ with $(x_1, x_2) \sim (y_1, y_2)$ if $x_1y_1 + x_2y_2 = 1$. In a similar way, if $d \geq 3$, take $\left(\mathbb{F}_p^d, \mathbb{F}_p^d, ..., \mathbb{F}_p^d\right)$ and for $x = (x_1, ..., x_d)$, $y = (y_1, ..., y_d)$,... We could define $(x, y, ...) \in H$ if $x_1y_1... + x_2y_2... + ...x_dy_d + ... = 1$. But this doesn't work for some reason!

Another idea: fix a $q = p^d$, $\mathbb{F}_p^d \approx \mathbb{F}_q$. Define $H = \mathbb{F}_q \times ... \times \mathbb{F}_q$ (d times) with $(a_1, ..., a_d) \in \mathbb{F}_q$ edge if $tr(a_1, ..., a_d) = 1$ where the trace

$$tr : \mathbb{F}_q \mapsto \mathbb{F}_p,\ tr(x) = x + x^p + x^{p^2} + ... + x^{p^{d-1}}.$$

The motivation for this is that tr is a multilinear function, which seamed necessary for the $d = 2$ case. Turns out this more clever graph does not have $K_{2...2}$. The size is $|H| = q^d/p = n^{d-\frac{1}{d}}$, which for $d = 2$ is the same (so is tight) and for $d = 3$, we get $3 - \frac{1}{3}$ which is better than the random one!

Proof. (of no $K_{2...2}$) suppose $a_i, b_i \in \mathbb{F}_q$. Then $tr(x_1, ...\, x_d) = 1$ for $x_i \in \{a_i, b_i\}$. Then look at

$$\begin{aligned}
&- tr(a_1, ..., a_i, ..., a_d) = 1\\
&+ tr(a_1, ..., b_i, ..., a_d) = 1\\
&= -tr(a_1, ..., (b_i - a_i), ...\, a_d) = 0 \quad \forall i
\end{aligned}$$

so let $b_i = a_i(1 + y_i)$ then $b_i - a_i = a_iy_i$. We know that $tr(A) = 1$, but $tr(Ay_i) = 0$ where $A = (a_1, ...\, a_i, ...\, a_d)$. But replacing two fixed elements, we have

$$\begin{aligned}
&+ tr(a_1, ..., a_i, ...\, a_j, ..., a_d) = 1\\
&- tr(a_1, ..., a_i, ...\, b_j, ..., a_d) = 1\\
&- tr(a_1, ..., b_i, ...\, a_j, ..., a_d) = 1\\
&+ tr(a_1, ..., b_i, ...\, b_j, ..., a_d) = 1\\
&= tr(a_1, ..., (b_i - a_i), ...\, (b_j - a_i), ...\, a_d) = 0
\end{aligned}$$

repeating this several times, it eventually tells us that $tr(Ay_{i_1}...y_{i_t}) = 0$ for any $i_1 < ... < i_t$. Now, $1,\ y_1,\ y_1y_2, \dots,\ y_1y_2...y_d \in \mathbb{F}_q \approx (\mathbb{F}_p)^d$ are all linearly dependent. This implies that there exist $c_0, c_1, \dots, c_d \in \mathbb{F}_p$ such that

$$c_0y_1 + c_2y_1y_2 + ... = 0\,. \tag{4.2}$$

Multiplying by A, and taking trace (which is linear), we have

$$c_0tr(A) + c_1tr(Ay_1)c_dtr(Ay_2) + ... = 0 \tag{4.3}$$

but all that stuff is 0 except the first term. So $c_0 = 0$. You can then divide by y_1 and repeat to see that $c_1 = 0$, and so on, which is a contradiction. □

Theorem 4.1 (Conlon, Polenton, Z.)**.** *There are H that are $K^{(d)}_{2...2}$-free and*

$$|H| \geq n^{d - \frac{1}{\lceil \frac{2^d-1}{d} \rceil}}\,. \tag{4.4}$$

So they have added the ceiling function. It is an exercise to show that $\forall d \geq 2$, $\frac{2^d-1}{d} \notin \mathbb{Z}$. The construction is for $V = \mathbb{F}_p^s$ and $T : V \times ... \times V \mapsto \mathbb{F}_p$ multilinear. The function itself is created randomly...

Define $H = \{(x_1, \dots, x_d) : T(x_1, \dots, x_d) = 1\}$. What is the edge set size? it is $\mathbb{E}\,|H| = \frac{1}{p}\,|V|^d$. For estimating the number of $K_{2...2}$ recall that your edges needed to be independent. In a fixed $K_{2...2}$, edges are still independent!

If x_i, y_i aren't collinear for all i, then the probability $\mathbb{P}\left[x_1y_1, \dots, x_dy_d \text{ form } K^{(d)}_{2...2}\right] = p^{-2^d}$. After a linear transform, we can assume that $x_i = (1, 0, 0, \dots, 0)$ and $y_i = (0, 1, 0, \dots, 0)$ for all i. The randomness: T is determined by its action on unit vectors. So the value of $T(e_{i_1}, \dots, e_{i_d})$ for each $i_1, \dots, i_d$ where e_i is a basis for V is chosen randomly, and this definition is uniformly random and does not depend on the basis chosen.

Otherwise, it could be that $x_i = \lambda y_i$ for some i, but this implies that there is no $K^{(d)}_{2...2}$. The reason is that $\lambda T(x_1, \dots, x_i, \dots, x_d) = T(x_1, \dots, y_i, \dots, x_d)$, and these cannot both be 1. This logic breaks down for $d \geq 3$...?

Therefore, at last we have $\mathbb{E}\#K^{(d)}_{2...2} = |V|^{2d} \cdot p^{-2^d}$ with $p = \frac{1}{p}$ (these are different p's...). This is not any better than before!? But the point is that now the $K^{(d)}_{2...2}$ "cluster" together. If $x_1, \dots, x_d$ and $y_2, \dots, y_d$ form $K^{(d)}_{2...2}$, then the lines joining x_i to y_i actually have lots more $K^{(d)}_{2...2}$ on them, so we can delete edges much more efficiently.

$$T(...\ tx_i + (1-t)y_i\ ...) = tT(...) + (1-t)T(...)$$

Lecture 5 – *Incidence Geometry 1* – Cosmin Pohoata

Let $P \subset \mathbb{R}^2$ and L a set of lines in $\mathbb{R}^2$. How many incidences can there be?

$$I(P, L) = \#\left\{(x, \ell) \in P \times L : x \in \ell\right\} \tag{5.1}$$

A trivial observation: $I(P, L) \leq |P||L|$. As a warm up, we can say that $I(P, L) \leq |P|^2 + |L|$. Also $I(P, L) \leq |P| + |L|^2$. To see this, split the line set into the lines that contain at most one point from P, and the ones that contain at least 2. The first creates $\leq |L|$ incidences. It is an exercise to show that the second set of lines creates at most $|P|^2$ incidences.

Slightly better, we know $I(P,L) \leq |P||L|^{1/2} + |L|$ (and, the same with roles swapped). You can prove this with an incidence graph if you want, since it has no $K_{2,2}$. This implies $I(P,L) \leq z(|P|,|L|,K_{2,2}) \leq |P||L|^{1/2} + |L|$. This is optimal, just take $P = \mathbb{F}_{p^2}$, and $L =$ all lines in $\mathbb{F}_{p^2}$.

Alternatively, you can use Cauchy-Schwartz. Split up the point set into $|P_i| = \frac{|P|}{k}$ sized sets. Then we can do

$$I(P,L) = \sum_{i=1}^{k} I(P_i, L) \leq \sum_{i=1}^{k} \left[|P_i|^2 + |L| \right] = k \left[\frac{|P|^2}{k^2} + |L| \right]. \tag{5.2}$$

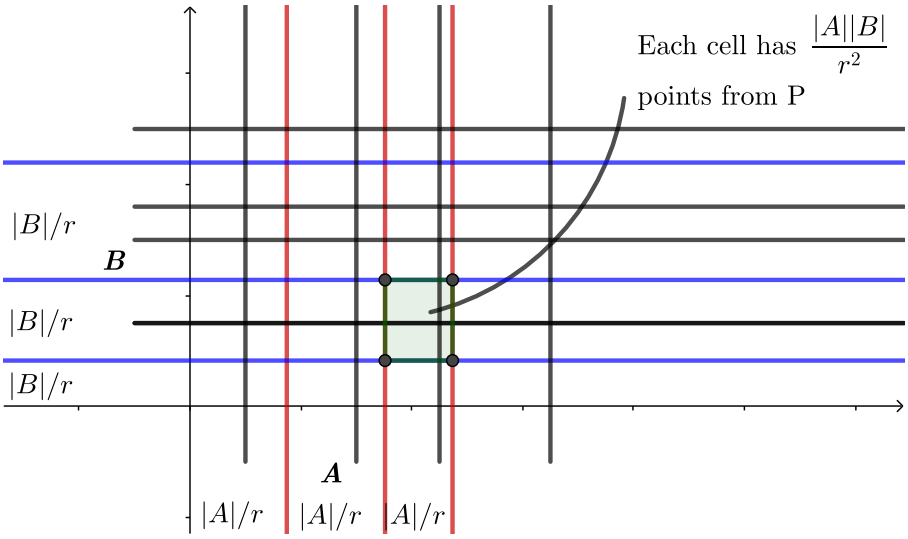
To balance these terms, we can choose $k \approx \frac{|P|}{|L|^{1/2}}$ to get the result. This choice of k only makes sense if $|P|^2 > |L|$, so that's why we have that error term of $+|L|$. This is another way to prove that $z(m,m,K_{2,2}) \leq mm^{1/2} + m$ (but with a worse constant). An open problem: can you use this partitioning argument for other things? Like to upper bound $z(m,m,m,K_{2,2,2})$?

Theorem 5.1 (Szemerédi Trotter, '83)**.** $I(P,L) \lesssim |P|^{2/3}|L|^{2/3} + |P| + |L|$

This theorem is interesting when $|P|^2 \geq |L| \geq |P|^{1/2}$. It is also optimal, there is a construction of m points and m lines in $\mathbb{R}^2$ with $\approx m^{4/3}$ incidences. Intuitively, we want to copy the sharp construction from $\mathbb{F}_p$ in a sense. So, we want a point and line set so that for lines $ax + b$, plugging in an x gives you something back in the set. Specificall, let's take $P = [k] \times [2k^2]$, and $L = \{\ell_{a,b} : a \in [k], b \in [k^2]\}$. Then $|P| = 2k^2$, $|L| = k^2 = m$. Each line has $\geq k$ points, so there are $m^{4/3}$ incidences.

Let's prove S.T. for grids... $P = A \times B$ for $A, B \subset \mathbb{R}$. The Motto for today is:

1. Divide P into pieces,
2. Apply a weaker lower bound for independent piece,
3. Add up contributions.



So, we split up the points into cells using axis parallel lines. Write $A = A_1 \sqcup A_2 \sqcup ... \sqcup A_r$ and $B = B_1 \sqcup B_2 \sqcup ... \sqcup B_r$ for $|A_i| = \frac{|A|}{r}$ and $|B_i| = \frac{|B|}{r}$. This is very clean with the grid-like set P,

since we can easily ensure that no points lie on our partitioning lines nor do they coincide with any of the line set. Then we can write

$$I(P,L) = \sum_{1\le i,j\le r} I(A_i \times B_j, L_{i,j}) \tag{5.3}$$

where $L_{i,j}$ is the set of lines hitting the cell with $A_i \times B_j$

$$I(A_i \times B_j, L) \le |A_i||B_j||L|^{1/2} + |L| = \frac{|A||B|}{r^2}|L|^{1/2} + |L| \tag{5.4}$$

so we have

$$\begin{aligned} I(P,L) &\le \sum_{1\le i,j,\le r} \frac{|A||B|}{r^2}|L|^{1/2} + |L_{i,j}| \\ &= \left(\frac{|A||B|}{r^2}\sum_{i,j}|L_{ij}|^{1/2}\right) + \sum_{i,j}|L_{ij}| \end{aligned} \tag{5.5}$$

With Cauchy Schwartz you can bound the first term with $r^{3/2}|L|^{1/2}$, using the fact that it's easy to bound the second term with $2\,|L|\,r$, which will get you there with the special choice of $r = \frac{|A|^{2/3}|B|^{2/3}}{|L|^{1/3}}$.

Lecture 6 – *Incidence Geometry 2* – Cosmin Pohoata

Sum-product problem: Given a finite set $A \subset \mathbb{R}$, How small can $\max\{|AA|, |A+A|\}$ be? Each of them could individually be as low as $2|A|-1$ and as large as $|A|^2$. Erdős and Szemerédi conjectured that for any set of real numbers, $\max\{|AA|, |A+A|\} \gtrsim |A|^{2-o(1)}$. Those two got the ball rolling and proved that $\max\{|AA|, |A+A|\} \gtrsim |A|^{1+c}$ for some $c > 0$.

Theorem 6.1 (Elekes, '96)**.** *For any $A \subset \mathbb{R}^2$,* $\max\{|AA|, |A+A|\} \gtrsim |A|^{5/4}$.

Proof. Create the grid again with $A+A$ on one edge and $A \cdot A$ on the other. We now define lines by $\ell_{ij} = a_i(x - a_j)$. For every pair, we get a distinct line, so there are n^2 of these lines. Then these lines are all n-rich, as ℓ_{ij} contains $(a_k + a_j, a_i a_k)$ for any k. Using the previous theorem now, we see $n^2 \le c\frac{(|A+A||A\cdot A|)^2}{n^3}$, so then $cn^{5/2} \le |A+A|\,|A\cdot A|$. □

The current record on this problem is By Rudnev-Stevens, (following a breakthrough of Solymosi) that $\max\{|AA|, |A+A|\} \gtrsim |A|^{\frac{4}{3}+\frac{2}{1167}-o(1)}$

The most elegant proof of Szemerédi-Trotter is due to Székely using the crossing number.

Proof. Without loss of generality, we can assume that each line contains at least 3 of the points as the lines with fewer contribute at most $2m$ incidences.

A line with k points can be separated into $k-1$ line segments, and since there are at least 3 points on each line there are at least 2 segments. This means $k - 1 \ge \frac{k}{2}$, and summing over all lines, the number of these segments is proportional to the number of incidences.

Consider the graph formed by taking the points as vertices, and the segments as edges. Since any two segments can intersect at most once, the crossing number of this graph is at most $\frac{m(m-1)}{2}$. The *crossing number inequality* implies that the number of edges e is bounded by $e \le 7n$, or that $\frac{m(m-1)}{2} \ge \frac{e^3}{29n^2}$. In either case, $e \lesssim (nm)^{2/3} + n + m$. □

Algebraic Approach time (Guth-Katz). Main idea: polynomial partitioning. Let $P \subseteq \mathbb{R}^d$, and let $r > 1$ (to be chosen later). Then, there is a polynomial in d variables $f \in \mathbb{R}[x_1, \ldots, x_d]$ such that $\deg g \leq r$ and $\mathbb{R}^d \backslash Z(f)$ is the disjoint union of cells each containing $\lesssim \frac{|P|}{r^d}$ points from P. This is called an r-partitioning polynomial. If you would like to read this proof, the best place to do that I know of is Terrence Tao's blog post about it: `https://terrytao.wordpress.com/2011/02/18/the-szemeredi-trotter-theorem-via-the-polynomial-ham-sandwich-theorem/`

Theorem 6.2 (Milma-Thom/Warren)**.** *If $f \in \mathbb{R}[x_1, \ldots, x_d]$, and $\deg g \lesssim r$, then $Z(f)$ splits $\mathbb{R}^d$ into at most $\lesssim r^d$ cells.*

Proving this is a good exercise in the case that $d = 2$. At this point, observe that what we did in the proof of Cartesian product Szemerédi-Trotter was basically this, we took our polynomial to be a collection of r axis parallel lines and we did obtain $\approx r^2$ cells.

Lecture 7 – *Pseudorandom Graphs 1* – David Conlon

Definition 7.1. *A graph G is (p, β)-jumbled if, for all $X, Y \subseteq V(G)$,*

$$|x(X,Y) - p|X||Y|| \leq \beta\sqrt{|X||Y|} \tag{7.1}$$

For a random graph, $e(X, Y)$ has expectation $p|X||Y|$ and deviation $\sqrt{p(1-p)|X||Y|}$.

Theorem 7.2. *If $p = p(n) \leq 0.99$, then W.H.P., $G(n, p)$ has that, for every $X, Y \subseteq V(G)$,*

$$|x(X,Y) - p|X||Y|| \leq c\sqrt{pn}\sqrt{|X||Y|} \tag{7.2}$$

i.e., W.H.P., $G(n, p)$ is $(p, c\sqrt{np})$-jumbled, so random graphs are pseudorandom. That is good. ("Best possible"?)

Definition 7.3. *If $q \equiv 1 \mod 4$, the Paley graph P_q with $V(P_q) = \mathbb{Z}/q\mathbb{Z}$, where $xy \in E(G)$ iff $x - y$ is a quadratic residue/square.*

Theorem 7.4. *Actually P_q is $(\frac{1}{2}, c\sqrt{q})$-jumbled.*

We defined the adjacency matrix, $A_{ij} = \begin{cases} 0 & \text{if } ij \notin E(G) \\ 1 & \text{if } ij \in E(G) \end{cases}$. There are real eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, and eigenvectors $v_1, \ldots, v_n$ such that $v_i v_j = \delta_{i,j}$. If G was d-regular, then $\lambda_1 = d$ with the eigenvector $v_1 = \frac{1}{\sqrt{n}}(1, \ldots, 1)$ and $|\lambda_i| \leq d$ for all $i \neq 1$. In a random graph, you would have largest eigenvalue of pn, and all others would be smaller – like $\sqrt{pn}$. The following Lemma relates these concepts; the eigenvalues really do tell you about (pseudo) randomness

Lemma 7.5 (Expander mixing)**.** *If G is an (n, d, λ)-graph (n vertices, d regular, $|\lambda_1| \leq \lambda$ for all $i \neq 1$) and $X, Y \subseteq V(G)$, then*

$$\left| e(X,Y) - \frac{d}{n}|X||Y| \right| \leq \lambda\sqrt{|X||Y|} \tag{7.3}$$

Proof. Let $B = \{v_1, \dots, v_n\}$ be an orthonormal basis of $\mathbb{R}^n$ consisting of eigenvectors of A where $Av_i = \lambda_i v_i$, $\lambda_1 = d$. In particular,

$$\begin{aligned} A_1 &= \lambda_1 \\ A_2 &= \sum_{i=2}^{d} \lambda_i v_i v_i \end{aligned} \tag{7.4}$$

Let $\chi_X \in \mathbb{R}^n$ be the characteristic vector of X, with $(\chi_X)_i = \begin{cases} 0 & \text{if } i \notin X \\ 1 & \text{if } i \in X \end{cases}$ and defined χ_Y similarly. We can write them in terms of the basis,

$$\chi_X = \sum_{i=1}^{n} \alpha_i v_i \quad \chi_Y = \sum_{i=1}^{n} \beta_i v_i \,, \tag{7.5}$$

and then $v_j^T \chi_x = \sum_{i=1}^n \alpha_i v_i^T v_i = \alpha_j$, and similarly $\beta_j = \chi_Y^T v_j$. Therefore

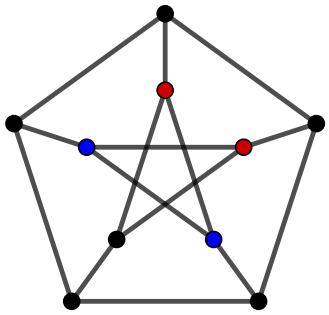
$$\begin{aligned} \sum_{i=1}^{n} \beta_j^2 &= \sum_{i=1}^{n} v_j^T \chi_Y \chi_Y^t v_j \\ &= \sum_{i=1}^{n} v_j^T \left|Y\right| v_j \\ &= |Y| \end{aligned}$$

Now, $e(X,Y) = \chi_C^T A \chi_Y$, so calculate $\chi_C^T A_1 \chi_Y$ and $\chi_C^T A_2 \chi_Y$ separately.

$$\begin{aligned} \chi_C^T A_1 \chi_Y &= \left(\sum_{i=1}^{n} \alpha_i v_i^T \right) \left(\lambda_1 v_1 v_1^T \right) \left(\sum_{j=1}^{n} \beta_j v_j^T \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j \lambda_1 (v_i^T v_1)(v_1^T v_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j \lambda_1 \delta_{i1} \delta_{1j} \\ &= \alpha_1 \beta_1 \lambda_1 \end{aligned}$$

and a similar computation leads to $\chi_X^T A_2 \chi_Y = \sum_{i=2}^n \alpha_i \beta_i \lambda_i$. Many computation later, and one application of Cauchy-Schwartz, we get there. □

Definition 7.6. *A graph is Strongly Regular with parameters (n, d, η, μ) if it as n vertices, is d=regular, and every pair of adjacent vertices has η common neighbours, and every pair of non-adjacent vertices has μ common neighbours.*



for example the petersen graph is $(10, 3, 0, 1)$*-strongly regular.*

Theorem 7.7. *The eigenvalues of an* (n, d, η, μ)*-strongly regular graph are* $\lambda_1 = d$ *with mult 1 and* $\lambda_2 = ...$ *with mult ...,* $\lambda_3 = ...$ *with mult ... (we decide to figure out what these should be during the proof)*

Proof. If A is the adjacency matrix, A^2 is the matrix where $(A^2)_{ij}$ measures the number of paths of length 2 from i to j. So the diagonal of A^2 is d in each entry. It will have η in every entry where $ij \in E(G)$, and μ when not. If J is the matrix of all ones, we can thus write

$$A^2 = \mu J + (d - \mu)I + (\eta - \mu)A.$$

Note also that since G is d-regular, $AJ = dJ$. We can now find the eigenvalues. $\lambda_1 = d$ with $v_1 = (1, 1, \dots, 1)$ and v_i for $i \neq 1$ is orthogonal to v_1. Therefore $Jv_i = 0$. Then

$$\begin{aligned} A^2 v_i &= \mu J v_i + (d - \mu)v_i + (\eta - \mu)Av_i \\ \lambda_i^2 &= (d - \mu) + (\eta - \mu)\lambda_i \end{aligned} \tag{7.6}$$

So we have a quadratic equation for all the eigevnalues,

$$\lambda^2 - (\eta - \mu)\lambda - (d - \mu) = 0 \tag{7.7}$$

which we can solve. You can ahead and for the multiplicities if you want too, you can write $1 + m_1 + m_2 = n$ and use $tr(A) = 0 = d + m_1\lambda_1 + m_2\lambda_2$ □

Exercise 7.8. p_q *is* $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right)$*-strongly regular. Using that and the previous theorem, we can find the eigenvalues*

$$\lambda = \frac{1 \pm \sqrt{q}}{2}. \tag{7.8}$$

By the expander mixing lemma, we have that if $X, Y \subseteq V(P_q)$, then

$$\left| e(X, Y) - \frac{1}{2}|X||Y| \right| \leq \frac{\sqrt{q} + 1}{2}\sqrt{|X||Y|} \tag{7.9}$$

Paley graphs are cool! We have a big conjecture, whose current bounds are:

$$\log q \log\log\log q \leq \omega(P_q) \leq \sqrt{q/2} \tag{7.10}$$

where the lower bound is for infinitely many q, not all q, and ω is the clique number. The conjecture is that the lower bound is closer to true.

Lecture 8 – *Pseudorandom Graphs 2* – Tibor Szabó

We restate the Expander Mixing Lemma,

Lemma 8.1 (Expander mixing)**.** *If G is an (n, d, λ)-graph (n vertices, d regular, $|\lambda_1| \leq \lambda$ for all $i \neq 1$), and $A, B \subseteq V(G)$, then*

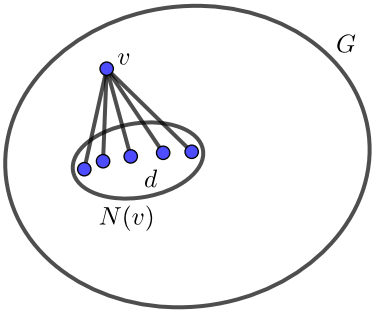
$$\left| e(X,Y) - \frac{d}{n}|A||B| \right| \leq \lambda\sqrt{|A||B|} \tag{8.1}$$

Recall that

$$e(A,B) = \#\left\{(a,b))a \in A, b \in B, an \in E(G)\right\} \tag{8.2}$$

One reason to study pseudorandom graphs is for explicit constructions. Eigenvalues provide an efficient way to verify. In applications, Pseudorandom graphs can be useful because they are not fully random. I.e., you can make local structures that do not appear in random graphs but globally the graph behaves randomlike.

For example, what do we know about K_3-free pseudorandom graphs? In random graphs, you can only have $\Theta(n)$ edges before you see a K_3. How dense can the pseudorandom ones be?



We compute using the expander mixing lemma,

$$\left| e(N(v), N(v)) - \frac{d \cdot d \cdot d}{n} \right| \leq \lambda\sqrt{dd} \tag{8.3}$$

And so

$$e(N(v), N(v)) \geq \frac{d^3}{n} - \lambda d > 0 \tag{8.4}$$

so $\frac{d^2}{n} > \lambda$.

Exercise 8.2. *For a (n, d, λ)-graph, $d \leq \frac{n}{2}$, then $\lambda = \Omega(\sqrt{(d)})$.*

so if $\lambda = \Theta(\sqrt{d})$, then G is "as pseudorandom" as possible. Paley for example is $\lambda = \Theta(\sqrt{n})$. So if this was true, we would have $\frac{d^2}{n} > \Theta(\sqrt{d} \iff d \leq \Theta(n^{2/2})$.

Alon is able to do this, getting a triangle free $(n, \Theta(n^{2/3}), \Theta(n^{1/3}))$, which in application gives $R(3,k) \geq k^{3/2}$ (the truth is that $R(3,k) \geq k^2/\log k$, but we don't know any explicit construction for that).

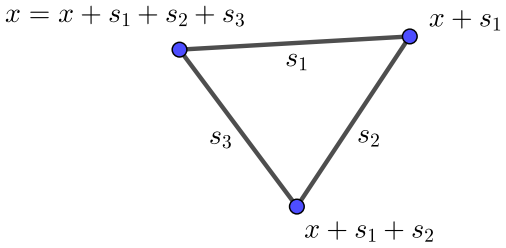
The construction we'll see is by Kopparty instead. We define the Cayley graph: $\langle H, + \rangle$, $S \subseteq H$, $S = -S$, $V(Cay(H,S)) = H$, and $E(Cay(H,S)) = \{\{x, x+s\} : x \in H, s \in S\}$ for $s = \{1, -1\}$.

We use this one since the Eigenvalues of $Cay(H,S)$ are described concretely through characters of H.

For our purposes, take $H = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ for p prime, and

$$S = \left\{ (xy, xy^2, xy^3) : y \in \mathbb{Z}_p^*, x \in \mathbb{Z}_p, \frac{p}{3} < x < \frac{2p}{3} \right\} \tag{8.5}$$

Observe that the Cayley graph is K_3-free $\iff$ for all $s_1, s_2, s_3 \in S$, $s_1 + s_2 + s_3 \neq 0$. To see this, look at this graph:



We have $x_1(y_1, y_1^2, y_1^3) + x_2(y_2, y_2^2, y_2^3) + x_3(y_3, y_3^2, y_3^3) = 0$, and if $y_1 = y_2 = y_3$, then $(x_1 + x_2 + x_3)(y, y^2, y^3) = 0$ but both of these are non-zero. If this is not the case, then you look at

$$\begin{bmatrix} y_1 & y_2 & y_3 \\ y_1^2 & y_2^2 & y_3^2 \\ y_1^3 & y_2^3 & y_3^3 \end{bmatrix} = 3 \tag{8.6}$$

The Vandermonde determinant is non zero, you can say those vectors are linearly independent which is a contradiction.

Now, let $x \in T \subset \mathbb{Z}_p \setminus \{0\}$ such that for all $x_1, x_2 x_3 \in T$ with $x_1 + x_2 + x_3$, we get $n = p^3 = |H|$ and $d = |S| = |T|(p-1) = \Omega(p^2)$ which we hope is equal to $\Omega(n^{2/3})$.

$\lambda << \frac{d^2}{n}$, $\lambda = \Theta(\sqrt{d}) \implies d >> n^{2/3}$ therefore $\exists$ many K_3. Further, $K_3 s$ are very well distributed all over the place in G. To measure this we can write

$$ex(G, K_3) = \text{max number of edges n a } K_3\text{- free subgraph of } G\,.$$

From Turán, $ex(K_n, K_3) = \lfloor \frac{n^2}{2} \rfloor$. In a random bipartite there is a bipartite subtraph with $\frac{e(G)}{2}$ edges.

Theorem 8.3. *For a (n, d, λ) graph G, and $\lambda << \frac{d^2}{n}$, we have $ex(G, K_3) = \left(\frac{1}{2} + o(1)\right) e(G)$.*

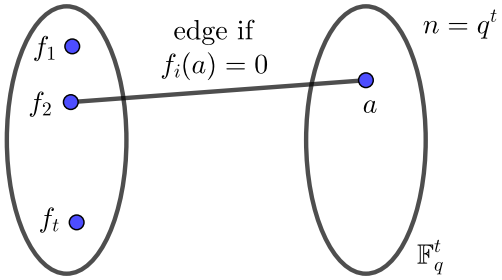
Lecture 9 – *Hypergraph Zarankiewicz 2* – Boris Bukh

We recapped the algebraic definitions from Lecture 3 and some additional basics.

Theorem 9.1 (Zarankiewicz construction)**.** *If $m \leq n^{\frac{s^{1/t}}{t^2}}$, then $z(n, m; s, t) \geq c_{s,t} m n^{1-\frac{1}{t}}$.*

E.g. if $m = n$ and $s = t^{2t}$.

Proof. For $j \le t$, call the collection of polynomials $f_{i_1}, f_{i_2}, \dots, f_{i_j}$ *good* if the dimension is what we expect, i.e. $\dim Z(f_{i_1}, f_{i_2}, \dots, f_{i_j}) = t-j$. Note that by definition $N(f_{i_1}, f_{i_2}, \dots, f_{i_j}) = Z(f_{i_1}, \dots, f_{i_j})$. If $j = t$ and it's good, then $\left|N(\dots) \cap \mathbb{F}_q^t\right| \le d^t$.



Induction: Take $f_1, \dots, f_{k-1}$, we want f_k. Pick $f_k \in P_d$ (polynomial of degree d). What's the probability that thee new collection is bad?

$$\mathbb{P}\left[f_{i_1}, f_{i_2}, \dots, f_{i_j}, f_k : bad\right] \tag{9.1}$$

Let $W = Z(f_{i_1}, f_{i_2}, \dots, f_{i_j})$, $\dim W = t - j$. By Lemma 3.6, $W \subseteq Z(f_k)$ or $\dim(W \cap Z(f_k)) = \dim W - 1$. Let $W = W_1 \cup \dots \cup W_M$ where W_i is irreducible, $\dim(W_k) \ge 1$. We have $M \le \prod_{\ell=1}^{j} \deg f_{i_\ell}$

Pick any $d+1$ points on W_k, $p_1, \dots, p_{d+1}$. We see

$$\mathbb{P}\left[Z(f_k) \cap W_k\right] \le \mathbb{P}\left[Z(f_k) \supseteq \{p_1, \dots, p_{d+1}\}\right] \le q^{-(d+1)} \tag{9.2}$$

where the last inequality is from Lemma 3.2. Thus

$$\mathbb{P}\left[\exists k \in Z(f_k) \supseteq W_k\right] \le d^t q^{-(d+1)} \tag{9.3}$$

so at last,

$$\mathbb{P}\left[f_{i_1}, f_{i_2}, \dots, f_{i_j}, f_k : bad\right] \le c q^{-(d+1)} \tag{9.4}$$

Hence,

$$\mathbb{P}\left[\text{some tuple is bad}\right] \le c \binom{k}{\le t-1} q^{-(d-1)} \tag{9.5}$$

and taking $m = cq^{\frac{d+1}{t-1}} = c\left(n^{1/t}\right)^{\frac{d+1}{t-1}} \ge cn^{\frac{d+1}{t^2}}$ and $d \approx t^2$ says that if $m = n$, $s = d^t = t^{2t}$. □

We missed something, which is to talk about the number of edges. We wave hands a bit, it follows from the face that a variety of $\dim d$ defined over $\mathbb{F}_q$ has $\approx q^d$ points.

Exercise 9.2. *Take a random polynomial f in 1 variable of degree d.*

1. $\mathbb{P}\left[f \text{ has } d \text{ roots}\right] = \frac{1}{d!}$
2. $$\mathbb{P}\left[f \text{ splits into factors of degree } a_1, a_2, \dots, a_t\right] = \frac{1}{|S_d|} \#\left\{\text{cycles in } S_d \text{ of cycle type } a_1, a_2, \dots, a_t\right\}$$

Want degree d because $s \leq d^t$, say $d = 3$. $\mathbb{F}_q^t$ is problematic because several points can lie on one line, among other degeneracies? So we replace $\mathbb{F}_q^t$ by $W = Z(g_1, \ldots, g_r) \cap \mathbb{F}_q^{t+r}$ where g_i are $(t+r)$-variate.

Definition 9.3. *For a variety W, $\{f|_W : f$ is a polynomial of degree $\leq d\}$ is a vector space. The Hilbert function $H_W(d)$ is the dimension over $\overline{\mathbb{F}}$ of that vector space.*

Examples:

1. $W = Z(x)$ in $\mathbb{R}^2$. This is a vertical line. The vector space is spanned by $1, y, y^2, \ldots, y^d$, so $H_W(d) = d + 1$.
2. if $W = Z(y - x^2)$... the vector space is spanned by $1, x, y, y^2, xy, y^3, xy^2, \ldots, y^d, xy^{d-1}$, so $H_W(d) = 2d + 1$.
3. $W = Z(\emptyset)$, the whole plane. This is spanned by all monomials of degree up to d, hence $H_w(d) = \binom{d+2}{2}$.

Fact: $H_W(d)$ is eventually a polynomial of degree $\dim W$.

Proposition 9.4. *f is sampled from P_d. Then $\mathbb{P}[Z(f) \supseteq W] \leq q^{-H_W(d)}$*

Exercise 9.5. *Suppose F is a subfield of K, and $V \subseteq K^m$ is a vector space over K, then $\dim_F (F^m \cap V) \leq \dim_K V$*

Lecture 10 – *Kakeya* – Boris Bukh

You can turn a unit line segment in the plane inside of an arbitrarily small area set. The Kakeya Problem is: what is the smallest set containing a line segment in every direction?

Theorem 10.1 (Besicovitch)**.** *Area (or volume in higher dims) =0 is possible.*

So that's solved... what about this: what is the smallest dimension of a Kakeya set in $\mathbb{R}^d$? The following conjecture is true in $\mathbb{R}^2$, and open otherwise.

Conjecture 10.2. *A Kakeya set has dimension at least d.*

Finite field Kakeya is the following. A set $K \subset \mathbb{F}_q^d$ is *Kakeya* if K contains a line in every direction. I.e., For all $b \in \mathbb{F}_q^d \setminus \{0\}$, there is an $a \in \mathbb{F}_q^d$ such that $\{a + dt : t \in \mathbb{F}_q\}$ is contained in K. We know $\mathbb{F}_q^r = r$. The "dim" of a set of q^r points is r. We conjecture that "dim" of $K = \log_q |K|$. There are clearly $|\mathbb{R}| + 1$ directions in $\mathbb{R}^2$, so it's safe to guess that there are $q + 1$ directions in $\mathbb{F}_q^2$. Thus $|K| \geq q + (q-1) + \ldots + 1 = \binom{q+1}{2}$, so K is 2 dimensional.

Theorem 10.3 (Dvir)**.** *If $K \subseteq \mathbb{F}_q^d$ is Kakeya then $|K| \geq \binom{q+d-1}{d}$ ($\approx \frac{q^d}{d!}$ for large q).*

Proof. Suppose $|K| < \binom{q+d-1}{d}$. We will look for a polynomial $f(x_1, \ldots, x_d)$ of degree $\leq q - 1$ that vanishes on K (i.e. $f(a) = 0$ for all $a \in K$). To do this, think of the $f(a) = 0$ as a linear equation in the coefficients of f. There are $\binom{q-1+d}{2}$ coeffs. $f(a) = 0$ furthermore is a homogeneous linear equation. There are $|K|$ equations, and since we assumed $|K| < \binom{q-1+d}{d}$, this system is underdetermined so there is a solution (there is such an $f \neq 0$).

Pick a $b \neq 0$, and let a be s.t. $\{a + bt : t \in \mathbb{F}_q\} \subseteq K$. Let $g_{a,b}(t) = f(a + bt)$. Then $g_{a,b}(t) = 0$ for all $t \in \mathbb{F}_q$, and the degree $\deg g_{a,b} \leq \deg f \leq q - 1$, which means $g_{a,b} = 0$ (in fact, every coef of $g_{a,b}$ is zero). Let $\deg f = k$. Split f up into $f = f_k + f_{k-1} + ... + f_0$ where f_i collects the terms of degree i in f. Each of the f_i are homogeneous with degree i.

The coefficient of t^k in $g_{a,b}$ is zero, so

$$\begin{aligned} 0 = [t^k]g_{a,b} &= [t^k]f(a + bt) \\ &= [t^k]f_k(a + bt) + [t^k]f_{k-1}(a + bt) + ... \end{aligned}$$

and every term in that sum is 0 except for $[t^k]f_k(a+bt)$. f_k contains terms like $cx_1^{e_1}x_2^{e_2}...x_d^{e_d}$, where $e_1 + ... + e_d = k$. We have

$$\begin{aligned} &[t^k]c(a_1 + b_1t)^{e_1}(a_2 + b_2t)^{e_2}...(a_d + b_dt)^{e_d} \\ &\qquad [t^k]c(b_1t)^{e_1}(b_2t)^{e_2}...(b_dt)^{e_d} \end{aligned}$$

and so

$$0 = [t^k]f = [t^k]f_k(a + bt) = [t^k]f_k(bt) = [t^k]t^k f_k(b) = f_k(b) \tag{10.1}$$

since b was arbitrary, f_k vanishes on every point of $\mathbb{F}_q^d$. It is an exercise to show that any polynomial of degree $\leq q - 1$ vanishing on $\mathbb{F}_q^d$ is the zero polynomial. This is a contradiction. □

So Dvir shows that $|K| \gtrsim \frac{q^d}{d!}$, but this was improved by B. and Chao to $|K| \gtrsim \frac{q^d}{2^{d-1}}$. An example is:

$$\left\{(a_1, a_2, ..., a_{d-1}) \in \mathbb{F}_q^d : a_i + b^2 \text{ is a square}\right\} \cup \{a_1, ..., a_{d-1}, 0 : a_i \in \mathbb{F}_q\} \tag{10.2}$$

That $|K| \gtrsim \frac{q^3}{4}$ *for* $k \in \mathbb{F}_q^3$. $f \in \mathbb{F}_q \in \mathbb{F}_q[x_1, ..., x_d]$ vanishes at $a = (a_1, ..., a_d)$ to order 2 if $f(a) = 0$ and $f(a + bt)$ has a double zero at $t = 0$ for all $b \neq 0$.

This condition is equivalent to saying that $f(x + a)$ has no constant term and no linear term. Let

$$A = \{(a_1, a_2, a_3) : 0 \leq a_1, a_2, a_3, \quad a_1 + a_2 + a_3 \leq 2q, \text{ and } a_1, a_2 \leq q - 1\}$$

define a vector space

$$V = \left\{\sum_{a \in A} c_{a_1a_2a_3}x_1^{a_1}x_2^{a_2}x_3^{a_3}\right\} \tag{10.3}$$

Look for $f \in V$ that vanishes at each $a \in K$ to order 2. There are $1 + 3$ linear equations on f for each point of K, the 1 coming from the constant term and the 3 coming from the three axes. If $\dim V > 4\,|K|$, then there is an $f \in V \setminus \{0\}$ satisfying this. An exercise is to show $|A| = q^3 + O(q^2)$ since this is just counting points on a polytope... If we find f, repeat Dvir's argument, looking at

$$g_{a,b}(t) = f(a + bt) \tag{10.4}$$

We see $\deg g_{a,b}(t) \leq \deg f \leq 2q - 1$, and $g_{a,b}(t)$ vanishes at every point to order 2, which means $g_{a,b} \equiv 0$, and similarly find that $f_k(b) = 0$ for every point in the space. We can use homogeneity to get

$$f_k(b_1, b_2, b_3) = b_3^k f_k\left(\frac{b_1}{b_3}, \frac{b_2}{b_3}, 1\right) \tag{10.5}$$

Now $f_k(x, y, 1)$ is a polynomial in x and y of degree $q - 1$ in each. □

Lecture 11 – *Szemerédi Trotter 3* – Dmitrii Zakharov

Recall from the previous lecture that we went through Szemerédi Trotter in the reals and used it to show some of the sum-product phenomenon. This may be because $\mathbb{R}$ has not subrings. In $\mathbb{F}_p$, Szemerédi Trotter is not true, as you can take P and L to be all of $\mathbb{F}_p^2$, and get $I(P,L) = p^3$ which is the Cauchy Schwartz bound.

What if $|P|, |L| < p^{2-c}$? Or what if $p = q^t$. Then $\mathbb{F}_q^2 \subset \mathbb{F}_p^2$, and we can take $P = \mathbb{F}_q^2$, $L =$ lines spanned by $\mathbb{F}_q^2$. This again gives $I(P,L) = |P|^{3/2}$. So let's sat p is a prime, but this makes the problem a bit harder since we need to use the distinction from p and p^2 somewhere.

Theorem 11.1. *If $|P| = |L| << p$, then $I(P,L) < |P|^{\frac{3}{2}-c}$ for some $c > 0$.*

This follows from a sum-product bound in $\mathbb{F}_p$. We want to show that for $A \subset \mathbb{F}_p$, $|A| < \sqrt{p}$, we have $\max\{|A+A|, |AA|\} > |A|^{1+c}$. The same problem is here, there is something special about being a prime and not a power of a prime.

Theorem 11.2 (Szőnyi)**.** *If p is a prime and $P \subset \mathbb{F}_p^2$ is a set of size $\leq p$, so that $P \not\subset$ line, then P determines at least $\frac{|P|}{2}$ distinct directions.*

This theorem is not true if $p = q^t$. you could take $P = \mathbb{F}_q^2$, which determine $q+1$ directions which is $<< q^2$.

We now talk about how to use this theorem to obtain the sum-product bound. Let $A \subset \mathbb{F}_p$, $|A| < p^{1/2}$. Then $A \times A \subset \mathbb{F}_p^2$. Then $\mathcal{A} \times A$ defines $\gtrsim |A|^2$ directions. For (a_1, a_2), $(b_1, b_2) \in A \times A$. We can define the directions by $s = \frac{a_1 - b_1}{a_2 - b_2}$. We we can write the directions like

$$\left| \frac{A-A}{A-A} \right| \geq |A|^2 \tag{11.1}$$

This inequality means that A cannot be a subring.

Additive combinatorics tells us that if $|AA| \leq K|A|$ and $|A+A| \leq K|A|$, then there is a subset A' of A with $|A'| > \frac{|A|}{K^C}$ so that any combinations of A' are also less than K^C. In particular, the combination

$$\left| \frac{A'-A'}{A'-A'} \right| < K^C |A'| \tag{11.2}$$

which implies $K > |A|^C$, and thats the end.

Some "polynomial stuff" can give you bounds for the number of points on a curve, i.e. take $f \in \mathbb{F}_p[x,y]$, $\deg f = d$, and $Z(f) = \{(x,y) \in \mathbb{F}_p^2 : f(x,y) = 0\}$. The Schwartz-Zippel Lemma says that $|Z(f)| \leq d \cdot p$, but you can improve this to $\frac{1}{2} d \cdot p$ if f has no linear factors (Steparov methods..?).

Another take on sum product: we have $A \subseteq \mathbb{F}_p$, look at $A + sA$ for some $s \in \mathbb{F}_p$. For many choices of s, $|A + sA| \geq |A|^2$, which means that $a + sa'$ are pairwise distinct. If $|A + sA| < |A|^2$, then for $a, a', b, b' \in A$, $a + sa' = b + sb'$, with $s = \frac{a-b}{a'-b'} \in \frac{A-A}{A-A}$.

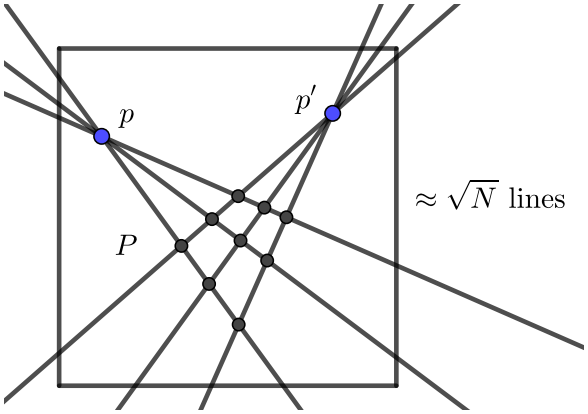
So $\frac{A-A}{A-A} \implies |A + sA| = |A|^2$. Idea: if we can find such an s inside some expression like $A \cdot A - ... + A \cdot A$, we will get $|A + (\text{that expression})A| \geq |A|^2$... we'll be good

"Punchline": $\mathbb{F}_p$ has no subgroups, so $\frac{A-A}{A-A}$ is not a subgroup. So there exists an $s \in \frac{A-A}{A-A}$, with $s + 1 \notin \frac{A-A}{A-A}$, thus

$$s + 1 = \frac{a_1 - a_2}{b_1 - b_2} + 1 = \frac{a_1 - a_2 + b_1 - b_2}{b_1 - b_2}\,, \tag{11.3}$$

so the expression we want is $\frac{A-A+A-A}{A-A}$.

Now back to Szemerédi Trotter. We have P, $L \subset \mathbb{F}_P^2$, with $|P| = |L| = N << p^2$. We want to show $I(P,L) < N^{\frac{3}{2}-c}$ for some $c > 0$. Idea: assume it's not so, $I(P,L) = N^{3/2}$. We will argue that then $\mathbb{F}_p$ contains something resembling a subfield, and use sum-product to get a contradiction.



If $I(P,L) = N^{3/2}$ then any line contains $\approx \sqrt{N}$ points, and every point is contained in $\approx \sqrt{N}$ lines. So take two points $p, p' \in P$. There are around $\sqrt{N}\sqrt{N} = N$ intersections. Each line has $\sqrt{N}$ pairs of P so there are around N points of P in those intersections. We now take a projective transformation, $p \mapsto (\infty, 0)$, $p \mapsto (0, \infty)$, We get a genuine grid.

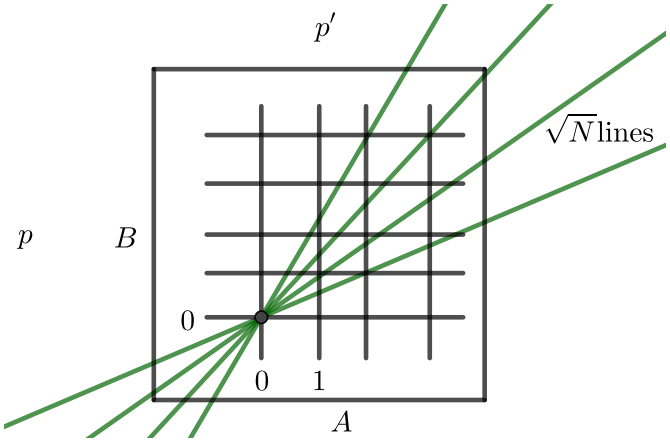


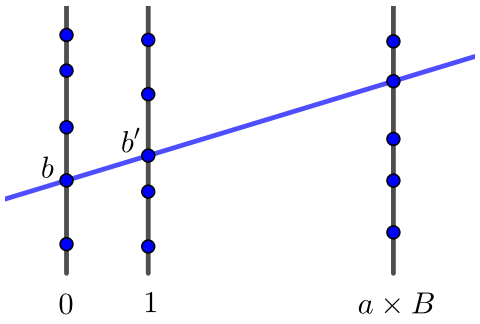
Figure 1

So we now have most of our point set in a cartesian product, $P \subseteq A \times B \subset \mathbb{F}_p^2$, with $|A|, |B| \approx \sqrt{N}$. L is also structured, most $\ell \in L$ have $(1, b'), (0, b) \in \ell$ for some $b, b' \in B$. So the line is

$$\ell = \ell_{b,b'} = \{(t, b + t(b' - b)) : t \in \mathbb{F}_p\} \tag{11.4}$$

For many pairs (b, b'), $\ell_{b,b'} \in L$, so there are around N choices.

Now, take $a \in A$, for many (b, b') : Line $\ell_{b,b'}$ contains (a, b'') iff $(a, b+a(b-b')) = (a, b'')$ for some $b'' \in B$. For fixed a, for many b, b', $b + a(b' - b) = b'' \in B$. We conclude that $(1 - a)B + aB \subset B$ (mostly) so B has small doubling, or $B + B$ is small.



Look at the green lines in Figure 1, $(-\{(t,bt) : t \in \mathbb{F}_p\}, b \in B)$. For most $b \in B$, $a \in A$, ℓ intersects $\{a\} \times B$, i.e. $(a, ab) \in \{a\} \times B$, so $ab \in B$ for most a, b in A, B. So, nearly, $AB \subset B$, so we have some multiplicative structure. Applying the Sum-Product result finishes things.

Lecture 12 – *Hypergraph Zarankiewicz 3* – Boris Bukh

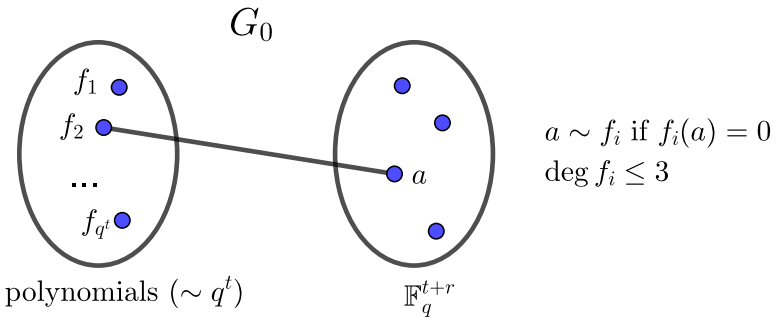
Let $W = t$-dimensional space. We could have that $H_W(d) = \binom{t+d}{d}$.

Lemma 12.1. *If W is a variety of dimension t, then $H_W(d) \geq \binom{t+d}{d}$.*

A (very rough) sketch of the proof... If you have any variety, you can pick a direction to project. You can pick a random (generic) direction in fact. Note that a variety projection to a hyperplane is still a variety.

Proof that $z(n,n;s,t) = \Omega(n^{2-\frac{1}{t}})$ if $s = 3^{t+o(t^{2/3}\log t)}$.

Phase 1: Let $r = 6t^{2/3}$. create a graph with edges of polynomials and elements of $\mathbb{F}_q^{t+r}$. $a \sim f_i$ if $f_i(a) = 0$, $\deg f_i \leq 3$. Call this graph G_0.



Phase 2: Cut down the right side of G_0. Replace $\mathbb{F}_q^{t+r}$ by $\mathbb{F}_q^{t+r} \cap (g_1, \dots, g_r) =: R$ for polynomials $g_1, \dots, g_r$ such that $Z(g_1, \dots, g_r)$ is t-dim (so that $|R| \sum q^t$). Then $N_G(f_1, \dots, f_t) = R \cap Z(f_1, \dots, f_t) = \mathbb{F}_q^{t+r} \cap Z(f_1, \dots, f_t, g_1, \dots, g_r)$. If this is 0 dimensional, this is of size $\leq \prod \deg f_i \prod \deg g_j = 3^t (t^2)^r = 3^{t+o(t^{2/3}\log t)}$.

Phase 1 (again?): $f_{i1}, \dots, f_{ij}$ are good if $\dim Z(f_{i1}, \dots, f_{ij}) = t + r - j$. We want that every set of at most t polynomials is good. We do induction on k. Suppose $f_1, \dots, f_{k-1}$ exist, f_k is sampled among $\deg \leq 3$ polys. Let M be the number of irreducible components of $Z(f_{i1}, \dots, f_{ij})$ which are

at most 3^t in number. Call them W_i. Then

$$\mathbb{P}\left[Z(f_{i1},\dots,f_{ij}) : \text{ is not cut}\right] \leq \sum_{i=1}^{M} \mathbb{P}\left[W_i \subseteq Z(f_k)\right] \leq \sum_i q^{-H_{W_i}(3)} \leq M q^{-\binom{t+r-j+s}{3}} \leq 3^t q^{-\binom{r+3}{3}} \leq 3^t q^{-36t^2} \tag{12.1}$$

We have the union bound:

$$t^3 \binom{m}{\leq t} q^{-36t^2} \leq \frac{3^t}{t!} \left(q^t\right)^t q^{-36t^2} \to 0 \tag{12.2}$$

very fast.

Phase 2 (again) Select $g_1,..,g_r$ inductively so that $Z(f_{i1},\dots,f_{ij},g_1,\dots,g_r)$ has dimension $t+r-t-k=r-k$. The probability that this fails,

$$\mathbb{P}\left[f_{i1},\dots,f_{ij},g_1,\dots,g_k \text{ fails this}\right] \leq q^{-t^2} \tag{12.3}$$

by "David's lemma". □

For Turán, we would want a single polynomial of degree 3, such that random polynomials $f_1 = f(x,y_1)$, $f_2 = f(x,y_2)$, ... are independent as random variables. But we can't quite do that. If you have 5 y_i on one line, then any cubic vanishing on 4 of them will also vanish on the 5th. So, we want no set of t points to be "3-dependent".

Definition 12.2. *$y_1,\dots,y_t$ are 3-independent if values of a random degree three polynomial at $y_1,\dots,y_t$ are independent random variables.*

We want to replace $\mathbb{F}_q^{t+r}$ by some W that contains no t-many 3-dependent elements with dimension $t+r$. How can we?? Well, take $\mathbb{F}_q^{t+r+\ell}$, and find random $h_1,\dots,h_\ell$ in $t+r+\ell$ variables such that $Z(h_1,\dots,h_\ell)$ contains no t 3-dependent sets. We want to

1. Count the 3-dependent sets
2. Bound $\mathbb{P}[S \subseteq Z(h_i)]$ for a 3-dependent S of size $|S| = t$

Point 2 is handled by the Hilbert function, with the following Lemma.

Lemma 12.3. *A set S is 3-dependent if $H_S(3) \leq |S| - 1$.*

To do point 1, we must count the number of solutions to $\ell_1(x)^3 + \dots + \ell_t(x)^3 = 0$ where ℓ_i are linear functions in $x = (x_1,\dots,x_{t+r+\ell})$.

Lecture 13 – *Slice Rank 1* – Dmitrii Zakharov

Idea of the rank method: in some problems you have a collection of objects $X_1,\dots,X_N$, and you are able to create a matrix which describes the relationship between the elements, $M = m_{ij}$ where $m_{i,j}$ quantifies the relationship between x_i and x_j.

1-distance sets in $\mathbb{R}^d$ (simplices). We have $x_1,\dots x_N$, and $\|x_i - x_j\| = 1$, what is the maximal N? We make the matrix $M = (||x_i - x_j||)_{i,j=1}^N$. This matrix is $J - I$, and $rkM \geq N - 1$. Also,

$||x_i - x_j||^2 = ||x_i||^2 + ||x_j||^2 - 2\langle x_i, x_j\rangle$. Making a matrix for each component, the first and second have rank 1, the third has rank $\sum_{x_{it}x_{jt}}$ each having rank one. So $rkM \leq 2 + d \implies N \leq d + 3$.

What about 2 distance sets? We have $x_1, \dots x_N$, and $\|x_i - x_j\| \in \{r, s\}$. The matrix $M = (||x_i - x_j||^2)_{ij}$ has 0 diagonal still but now a combo of r^2 and s^2 elsewhere. We can still show that $rkM \leq d + 2$, but it's hard to lower bound it. Let $f(u) = (s^2 - u)(r^2 - u)$. Applying this to every entry of the matrix, we get a diagonal one, which has rank $\geq N$. We also know

$$f(M_{ij}) = f(||x_i - x_j||^2) = (s^2 - ||x_i - x_j||^2)(r^2 - ||x_i - x_j||^2) = (s^2 - |x_i||^2 - ||x_j||^2 + 2\langle x_i, x_j\rangle)(r^2 - \dots)$$

Of all the terms present when you expand that, the only one that isn't easy to handle is the $\langle x_i, x_j\rangle^2$. Expanding this and doing some computation we get $rkf(M) \lesssim d^2$, and we already had $rkf(M) \geq N$, and so $N \lesssim d^2$. This is tight, as the example $x_i = (0, \dots, 0, 1, 0, \dots, 0, 1, 0, \dots, 0)$ shows... There are $\binom{d}{2}$ points like that with only 2 distances.

And application; if $A \subset [N]$ and A has no 3AP, how large can A be? Roth showed that $|A| = o(N)$, and this year (ask the names) proved $Ne^{-(\log N)^{1/11}}$. In the finite field version, $A \subset \mathbb{F}_3^n$ with no 3APs, the bound before was $|A| \leq \frac{3^n}{n^{1+c}}$, in '16 it was brought to $|A| \leq 2.9^n$.

Let $A \subset \mathbb{F}_3^n$ with no 3APs, and let $a, b, c \in A$, $2b = a + c$ iff $a + b + c = 0$ iff a, b, c are collinear and distinct. So if for all a, b, c distinct, $a + b + c \neq 0$ then there are no 3APs. We will call this the 3-uniform condition. The 2-uniform condition is that if $a \neq b$, $a, b \in A$ then $a + b \notin A$ and if $a = b$ then $a + b = -a \in -A$.

Defined the matrix $M = (a + b)_{a,b \in A}$ which is $|A| \times |A|$. You can see this has rank 2. Let's choose a function F and look at $F(M)$ again. We want $F(\text{off diagonal}) = 0$ and $f(\text{diag}) \neq 0$ often.

What is F? Lettuce choose it to be a polynomial of degree t,

$$P_t = \left\{ \sum x_1^{d_1} \dots x_n^{d_n} : d_i \leq 2, \sum d_i \leq t \right\} \tag{13.1}$$

Want to find $F \in P_t$ such that $F(\mathbb{F}_3^n \setminus -A) = 0$ and # non-zero $F(a), a \in A$ large.

It is an exercise to show that if $V \subset \mathbb{F}^n$ and $\dim V = d$, then there is a $v \in V$ with $\geq d$ non-zero coordinates. Let's use $V = \{F \in P_t : F(\mathbb{F}_3^n \setminus -A) = 0\}$. $\dim V = \dim P_t - (3^n - |A|)$. It's another exercise to show there exists $F \in P^t$, $F(-A) = 0$, $\#\{F(a) \neq 0\} \geq \dim P_t - (3^n - |A|)$. This implies $rkF(M) \geq \dim P_t - (3^n - |A|)$.

$$F(M)_{a,b} = F(a + b) = \sum_{\text{monomials } 0 \leq d_i \leq 2, \deg \leq t} c(a_1 + b_1)^{d_1} \dots (a_n + b_n)^{d_n} = \sum_{m, m', \deg m + \deg m' \leq t} m(a)m'(b) \tag{13.2}$$

How many terms are there? There are...

$$\sum_{m, m', \deg m + \deg m' \leq t} m(a)m'(b) = \sum_{\deg m \leq \frac{t}{2}} m(a)[\text{ stuff }] + m(b)[\dots] \leq 2 \dim P_{t/2} \tag{13.3}$$

$\dim P_t(3^n - |A|) \leq rkF(M) \leq 2 \dim P_{t/2}$. We want to make $\dim P_t$ large and $\dim P_{t/2}$ small. So if we take $t \in [d, 2d]$, $\dim P_t = 3^n - c^n$, $\dim P_{t/2} \leq c^n$, so $3^n - c^n - (3^n - |A|) \leq 2c^n$, hence $|A| \leq 3c^n$, and we can optimally make $c \approx 2.9$...

Lecture 14 – *Slice Rank 2* – Cosmin Pohoata

Given a field $\mathbb{F}$ and any finite set X, we say $T : X \times X \times X \mapsto \mathbb{F}$ has slice rank 1 if $T(x, y, z) = f(x)g(y, z)$ or $f(y)g(x, z)$ or (and so on). The slice rank of T is defined by $SR(T) = \min r : T = \sum_{i=1}^r T_i$, where $T_1, \dots, T_r : X^3 \mapsto \mathbb{F}$ have slice rank 1.

For example, $T(x,y,z) = x(y+z)$ has slice rank 1. The function $T(x,y,z) = xy+yz+zx$ has slice rank 2, since we can write it as $x(y+z)+yz$ which both have slice rank 1.

Lemma 14.1 (Main)**.** *If we have $T : X \times X \times X \mapsto \mathbb{F}$ such that $T(x,y,z) \neq 0$ iff $x = y = z$, then $SR(T) = |X|$.*

Proof. Observe that $SR(T) \leq |X|$. This is because

$$T(x,y,z) = \sum_{x_0 \in X} \delta(x,x_0) T(x_0,y,z)\,. \tag{14.1}$$

For the other direction, suppose there exists an $\ell < |X|$ such that

$$T(x,y,z) = \sum_{i=1}^{j} f_i(x) g_i(y,z) + \sum_{i=j+1}^{k} f_i(y) g(x,z) + \sum_{i=k+1}^{\ell} f_i(z) g(x,y)$$

Main idea: consider $V = \left\{v : X \mapsto \mathbb{F} : \sum_{x\in X} v(x) f_i(x) = 0 \;\forall\; i = 1,\dots,j\right\}$. Then $\dim V \geq |X| - j$. There is a $v \in V$ such that $|\operatorname{supp}(v)| \geq |X| - j$. To see this, look at $\Theta : V \mapsto \mathbb{F}^{|\operatorname{supp}(v)|}$, $v \mapsto (v(x))_{x \in |\operatorname{supp}(V)|}$. If $|\operatorname{supp}(v)| < |X| - j \leq \dim V$, then $ker\Theta$ is non-trivial, i.e. there is a nonzero $w \in V$ such that $w(x) = 0$ for all $x \in \operatorname{supp}(V)$. Look at $v + w$. $(v+w)(x) = v(x) \neq 0$ for all $x \in \operatorname{supp}(v)$.

Consider $\sum_{x\in X} v(x) T(x,y,z) := G(y,z)$. What can we say about the rank of G (the matrix rank, the $|X| \times |X|$ matrix with entries $G_{y,z} = G(y,z)$).

$$\sum_{x\in X} \sum_{i=1}^{j} v(x) f_i(x) g_i'(y,z) + \sum_{x\in X} \sum_{i=j+1}^{k} v(y) f_i(x) g_i'(x,z) + + \sum_{x\in X} \sum_{i=k+1}^{\ell} v(x) f_i(z) g_i'(x,y) \tag{14.2}$$

Notice that the first double sum is 0 after changing the order of summation and moving the $g_i(y,z)$ out (the sum $\sum_{x\in X} v(x) f_i(x) = 0$). Thus (14.2) becomes

$$\sum_{i=j+1}^{k} f_i(y) \cdot \sum_{x\in X} v(x) g_i(x,z) + \sum_{i=k+1}^{\ell} f_i(z) \cdot \sum_{x\in X} v(x) g_i(x,y) \tag{14.3}$$

Those inner sums are just functions of z and y alone, which we denote $h_i(z)$ and $h_i(y)$. Observe that $G(y,y) = \sum_{x\in X} v(x) T(x,y,y) = *$ which is 0 if $x \neq y$. if $y \in \operatorname{supp}(v)$, $* = v(y) \cdot T(y,y,y) \neq 0$, so this is a diagonal matrix. We have $|X| - j \leq |\operatorname{supp}(v)| = rk(G) \leq \ell - j$ which is a contradiction. □

If $A \subseteq \mathbb{F}_3^m$, A contains no nontrivial 3AP then $|A| \leq 2.756^m$. The main idea is that in $\mathbb{F}_3$, $1 - x^2 \neq 0$ iff $x = 0$. So take $T : A \times A \times A \mapsto \mathbb{F}_3$ s.t. $T(x,y,z) = \prod_{i=1}^{m} (1 - (x_i + y_i + z_i))$. Observe that $T(x,y,z) \neq 0$ iff $x+y+z = 0$ iff $x = y = z$ so in other words, this tensor is diagonal. $SR(T) = |A|$. Expand the equation for T with some compact notation ($|I| + |J| + |K| \leq 2m$, $I, J, K \in \{0,1,2\}^m$ where $x^I = x_1^{i_1} \dots x_m^{i_m}$),

$$\begin{aligned} T(x,y,z) &= \sum c_{I,J,K} x^I y^J z^K \\ &= \sum_{I \in \{0,1,2\}^m, |I| \leq \frac{2m}{3}} x^I g_I(y,z) + \sum_{J \in \{0,1,2\}^m, |J| \leq \frac{2m}{3}} y^J g_J(x,z) + \sum_{K \in \{0,1,2\}^m, |K| \leq \frac{2m}{3}} z^K g_K(x,y) \end{aligned} \tag{14.4}$$

So $SR(T) \leq 3 \cdot \#I \in \{0,1,2\}^m$ s.t. $i_1 + ... + i_m \leq \frac{2m}{3}$. Observe that

$$\#I \in \{0,1,2\}^m : i_1 + ... + i_m \leq t \leq \frac{(1+x+x^2)^m}{x^t}, \ \forall 0 < x \leq m \tag{14.5}$$

Look at $(i_1, ..., i_m) \mapsto x^{i_1+...+i_m-t} \geq 1$, $\Phi(x) = \frac{1+x+x^2}{x^{2/3}}$.

Erdős, Szemerédi : given a collection $\mathcal{F}$ of subsets of $\{1, ..., m\}$ such that there are no pairwise distinct sets X, Y, Z such that $X \cap Y = Y \cap Z = Z \cap X$. Is it true that $|\mathcal{F}| \leq c^m$ for some $c < 2$?

Theorem 14.2 (Naslund - Sawin)**.** $|\mathcal{F}| \leq 1.88^m$

Proof. Exercise. The hint is to consider $T : \{0,1\}^m \times \{0,1\}^m \times \{0,1\}^m \mapsto \mathbb{R}$, $T(x,y,z) = \prod_{i=1}^m (z - (x_1 + y_1 + z_i))$. □