Randomly piercing algebraic sets

joint with Daniel Altman

Georgia Tech Combinatorics Seminar

Setup

For an odd prime p and collection of polynomials $f_1, \ldots, f_s \in \mathbb{F}_p[x_1, \ldots, x_n]$ let

$$V = V(f_1, \ldots, f_s) = \left\{x \in \mathbb{F}_p^n : f_1(x) = \cdots = f_s(x) = 0\right\}$$

be a variety. We also say that V is generated by $f_1, \ldots, f_s$.

Setup

For an odd prime p and collection of polynomials $f_1, \ldots, f_s \in \mathbb{F}_p[x_1, \ldots, x_n]$ let

$$V = V(f_1, \ldots, f_s) = \left\{x \in \mathbb{F}_p^n : f_1(x) = \cdots = f_s(x) = 0\right\}$$

be a variety. We also say that V is generated by $f_1, \ldots, f_s$.

Say $M \subseteq \mathbb{F}_p^n$ pierces a collection $\mathcal{F}$ of subsets of $\mathbb{F}_p^n$ if

$$M \cap F \neq \emptyset, \quad \text{for all } F \in \mathcal{F}$$

Setup

For an odd prime p and collection of polynomials $f_1, \ldots, f_s \in \mathbb{F}_p[x_1, \ldots, x_n]$ let

$$V = V(f_1, \ldots, f_s) = \left\{x \in \mathbb{F}_p^n : f_1(x) = \cdots = f_s(x) = 0\right\}$$

be a variety. We also say that V is generated by $f_1, \ldots, f_s$.

Say $M \subseteq \mathbb{F}_p^n$ pierces a collection $\mathcal{F}$ of subsets of $\mathbb{F}_p^n$ if

$$M \cap F \neq \emptyset, \quad \text{for all } F \in \mathcal{F}$$

We are interested in how big of a random subset of $\mathbb{F}_p^n$ one must take to pierce some collection of algebraic sets with high probability (as n grows).

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Geometry: $\mathcal{F}$ consists of compact convex sets in $\mathbb{R}^d$

- Helly's theorem (1913) says that if every subcollection in $\mathcal{F}$ of size $d+1$ is $1-$piercable then so is $\mathcal{F}$.

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Geometry: $\mathcal{F}$ consists of compact convex sets in $\mathbb{R}^d$

- Helly's theorem (1913) says that if every subcollection in $\mathcal{F}$ of size $d+1$ is $1-$piercable then so is $\mathcal{F}$.
- (Alon–Kleitman, 1992) resolve the (p, q) question: For $p \geq q \geq d+1$ if among every p members of $\mathcal{F}$ some q are $1-$piercable then $\mathcal{F}$ is piercable by some finite set.

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Geometry: $\mathcal{F}$ consists of compact convex sets in $\mathbb{R}^d$

- Helly's theorem (1913) says that if every subcollection in $\mathcal{F}$ of size $d+1$ is $1-$piercable then so is $\mathcal{F}$.
- (Alon–Kleitman, 1992) resolve the (p, q) question: For $p \geq q \geq d+1$ if among every p members of $\mathcal{F}$ some q are $1-$piercable then $\mathcal{F}$ is piercable by some finite set.

Graphs: $\mathcal{F}$ consists of maximum independent sets

- (Bollobás–Erdős–Tuza, $\leq$ 1994) conjecture that a sublinear number of vertices suffice to pierce $\mathcal{F}$ if $\alpha(G)$ is linear.

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Geometry: $\mathcal{F}$ consists of compact convex sets in $\mathbb{R}^d$

- Helly's theorem (1913) says that if every subcollection in $\mathcal{F}$ of size $d+1$ is $1-$piercable then so is $\mathcal{F}$.
- (Alon–Kleitman, 1992) resolve the (p, q) question: For $p \geq q \geq d+1$ if among every p members of $\mathcal{F}$ some q are $1-$piercable then $\mathcal{F}$ is piercable by some finite set.

Graphs: $\mathcal{F}$ consists of maximum independent sets

- (Bollobás–Erdős–Tuza, $\leq$ 1994) conjecture that a sublinear number of vertices suffice to pierce $\mathcal{F}$ if $\alpha(G)$ is linear.
- Progress in special cases (regular, free of large induced matchings, etc).

Piercing

Collection of subsets $\mathcal{F}$ is $k-$piercable if there exists $|M| = k$ which pierces $\mathcal{F}$.

Geometry: $\mathcal{F}$ consists of compact convex sets in $\mathbb{R}^d$

- Helly's theorem (1913) says that if every subcollection in $\mathcal{F}$ of size $d+1$ is $1-$piercable then so is $\mathcal{F}$.
- (Alon–Kleitman, 1992) resolve the (p, q) question: For $p \geq q \geq d+1$ if among every p members of $\mathcal{F}$ some q are $1-$piercable then $\mathcal{F}$ is piercable by some finite set.

Graphs: $\mathcal{F}$ consists of maximum independent sets

- (Bollobás–Erdős–Tuza, $\leq$ 1994) conjecture that a sublinear number of vertices suffice to pierce $\mathcal{F}$ if $\alpha(G)$ is linear.
- Progress in special cases (regular, free of large induced matchings, etc).

Arithmetic geometry: $\mathcal{F} = \left\{V(f) : f(x) = x^\top Ax, A \in \mathrm{Mat}_n(\mathbb{F}_p)\right\}$. How many (random) points to pierce?

Main result

Theorem (Threshold, Altman–T. 2026++)

Let $M \subset \mathbb{F}_p^n$ be a set chosen **uniformly at random** *among sets of fixed size $|M|$.*

Main result

Theorem (Threshold, Altman–T. 2026++)

Let $M \subset \mathbb{F}_p^n$ be a set chosen **uniformly at random** *among sets of fixed size $|M|$. Let $\mathcal{F}_{k,s}$ be the collection of nonempty varieties determined by the vanishing of s* **polynomials** *which each have* **degree at most** *$k \geq 2$.*

Main result

Theorem (Threshold, Altman–T. 2026++)

Let $M \subset \mathbb{F}_p^n$ be a set chosen **uniformly at random** *among sets of fixed size $|M|$. Let $\mathcal{F}_{k,s}$ be the collection of nonempty varieties determined by the vanishing of s* **polynomials** *which each have* **degree at most** *$k \geq 2$. Then letting*

$$c_{k,s} = \frac{p^{(s-1)k} \log p}{\log(1 + (p-1)^{-1})},$$

we have for every $\varepsilon > 0$

$$\mathbb{P}(M \text{ pierces } \mathcal{F}_{k,s}) = \begin{cases} 1 - o(1), & |M| \geq (c_{k,s} + \varepsilon)\binom{n}{k} \\ o(1), & |M| \leq (c_{k,s} - \varepsilon)\binom{n}{k} \end{cases},$$

as $n \to \infty$.

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$:

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$: For every $\alpha > 0$ and $A \subseteq G$ with $|A| \geq \alpha|G|$,

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$: For every $\alpha > 0$ and $A \subseteq G$ with $|A| \geq \alpha|G|$, there exists $d \in M$ and $x, x + d, \ldots, x + (k-1)d \in A$.

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$: For every $\alpha > 0$ and $A \subseteq G$ with $|A| \geq \alpha|G|$, there exists $d \in M$ and $x, x + d, \ldots, x + (k-1)d \in A$.

- For $G = M = \mathbb{Z}_N$ Roth established $k = 3$ in 1953, Szemerédi general k in 1975.

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$: For every $\alpha > 0$ and $A \subseteq G$ with $|A| \geq \alpha|G|$, there exists $d \in M$ and $x, x + d, \ldots, x + (k-1)d \in A$.

- For $G = M = \mathbb{Z}_N$ Roth established $k = 3$ in 1953, Szemerédi general k in 1975.
- Sparse M with special structure, ex polynomial sequences (Bergelson–Leibman, 1996)

Random Szemerédi: setup

Say Szemerédi's theorem holds for k-APs with common differences in M if the following holds for sufficiently large N and abelian $|G| = N$: For every $\alpha > 0$ and $A \subseteq G$ with $|A| \geq \alpha|G|$, there exists $d \in M$ and $x, x + d, \ldots, x + (k-1)d \in A$.

- For $G = M = \mathbb{Z}_N$ Roth established $k = 3$ in 1953, Szemerédi general k in 1975.
- Sparse M with special structure, ex polynomial sequences (Bergelson–Leibman, 1996)

What if M is random? Let $\delta_k^G = \delta_{\alpha,k}^G(N)$ be the probability threshold function for Szemerédi's theorem holding with differences in M, sampling $M \subseteq G$ with $|M| = \delta_k^G$.

Random Szemerédi: integers

Upper bounds in $[N]$

- (Bourgain, 1987) $\delta_2^I \lesssim \log N$

Random Szemerédi: integers

Upper bounds in $[N]$

- (Bourgain, 1987) $\delta_2^I \lesssim \log N$
- (Frantzikinakis–Lesigne–Wierdl, 2012) $\delta_3^I \leq N^{\frac{1}{2}+o(1)}$

Random Szemerédi: integers

Upper bounds in $[N]$

- (Bourgain, 1987) $\delta_2^I \lesssim \log N$
- (Frantzikinakis–Lesigne–Wierdl, 2012) $\delta_3^I \leq N^{\frac{1}{2}+o(1)}$
- (Briët–Dvir-Gopi, 2019) $\delta_k^I \leq N^{1-\frac{1}{\lceil k/2 \rceil}+o(1)}$ for all $k \geq 2$

Random Szemerédi: integers

Upper bounds in $[N]$

- (Bourgain, 1987) $\delta_2^I \lesssim \log N$
- (Frantzikinakis–Lesigne–Wierdl, 2012) $\delta_3^I \leq N^{\frac{1}{2}+o(1)}$
- (Briët–Dvir-Gopi, 2019) $\delta_k^I \leq N^{1-\frac{1}{\lceil k/2 \rceil}+o(1)}$ for all $k \geq 2$
- (Briët–Castro-Silva, 2024) $\delta_k^I \leq N^{1-\frac{2}{k}+o(1)}$ for all $k \geq 2$

Random Szemerédi: integers

Upper bounds in $[N]$

- (Bourgain, 1987) $\delta_2^I \lesssim \log N$
- (Frantzikinakis–Lesigne–Wierdl, 2012) $\delta_3^I \leq N^{\frac{1}{2}+o(1)}$
- (Briët–Dvir-Gopi, 2019) $\delta_k^I \leq N^{1-\frac{1}{\lceil k/2 \rceil}+o(1)}$ for all $k \geq 2$
- (Briët–Castro-Silva, 2024) $\delta_k^I \leq N^{1-\frac{2}{k}+o(1)}$ for all $k \geq 2$

Conjecture (Frantzikinakis–Lesigne–Wierdl, 2016)

$\delta_k^I \asymp \log N$ *for all* $k \geq 2$

Random Szemerédi: finite fields

In finite fields the story is quite different

Theorem ($k = 3$ Altman 2020, Briët 2021, Zheng 2025+)

There exists C such that, with $N = p^n$

$$\begin{aligned}\delta_k^F &\geq \binom{n+k-2}{k-1} - C(\log_p n)^{1+o(1)} n^{k-2} \\ &\geq \left(\frac{1}{(k-1)!} + o(1)\right) (\log_p N)^{k-1}\end{aligned}$$

Random Szemerédi: finite fields

In finite fields the story is quite different

Theorem ($k = 3$ Altman 2020, Briët 2021, Zheng 2025+)

There exists C such that, with $N = p^n$

$$\begin{aligned}\delta_k^F &\geq \binom{n+k-2}{k-1} - C(\log_p n)^{1+o(1)} n^{k-2} \\ &\geq \left(\frac{1}{(k-1)!} + o(1)\right) (\log_p N)^{k-1}\end{aligned}$$

Conjecture (Folklore)

$\delta_k^F \asymp (\log_p N)^{k-1}$ *for* $k \geq 2$

Random Szemerédi

Theorem (Altman–T. 2026++)

Let $\alpha = p^{-(t+1)}$. Then

$$\begin{aligned}\delta^F_{\alpha,K} &\geq (1-o(1))\frac{\log(p^t)}{\log(1+(p^t-1)^{-1})(k-1)!}\left(\log_p N\right)^{k-1}\\ &= \left(1-o_{\substack{\alpha\to 0\\ n\to\infty}}(1)\right)\frac{\alpha^{-1}\log\alpha^{-1}}{p}\frac{1}{(k-1)!}\left(\log_p N\right)^{k-1}.\end{aligned}$$

Random Szemerédi

Theorem (Altman–T. 2026++)

Let $\alpha = p^{-(t+1)}$. *Then*

$$\delta^F_{\alpha,K} \geq (1-o(1))\frac{\log(p^t)}{\log(1+(p^t-1)^{-1})(k-1)!}\left(\log_p N\right)^{k-1}$$
$$= \left(1-o_{\substack{\alpha\to 0\\ n\to\infty}}(1)\right)\frac{\alpha^{-1}\log\alpha^{-1}}{p}\frac{1}{(k-1)!}\left(\log_p N\right)^{k-1}.$$

On the other hand, if

$$|M| = \omega\left((\log N)^{k-1}\right)$$

then with high probability every **variety** V *with* $|V| = \Omega(N)$ **contains a** k**-AP** *with common difference in* M.

Proof of Random Szemerédi Application

If f is homogeneous of degree k then

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}f(x+jd) = \Delta_d^k f(x) = \Delta_d^k f(0) = k!f(d).$$

Proof of Random Szemerédi Application

If f is homogeneous of degree k then

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}f(x+jd) = \Delta_d^k f(x) = \Delta_d^k f(0) = k!f(d).$$

So if $x, x+d, \ldots, x+kd \in V(f)$ then also $d \in V(f)$.

Proof of Random Szemerédi Application

If f is homogeneous of degree k then

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}f(x+jd) = \Delta_d^k f(x) = \Delta_d^k f(0) = k!f(d).$$

So if $x, x+d, \ldots, x+kd \in V(f)$ then also $d \in V(f)$.

Lower bound follows from **disjoint variety** generated by t polynomials.

Proof of Random Szemerédi Application

If f is homogeneous of degree k then

$$\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}f(x+jd) = \Delta_d^k f(x) = \Delta_d^k f(0) = k!f(d).$$

So if $x, x+d, \ldots, x+kd \in V(f)$ then also $d \in V(f)$.

Lower bound follows from **disjoint variety** generated by t polynomials.

Upper bound follows by fact that **any variety** in $\mathbb{F}_p^n$ can be generated by at most n polynomials.

Analytic Rank

The analytic rank (Gowers–Wolf, 2011) of a polynomial f of degree k is

$$r(f) = -\log_p \left| \mathbb{E}_{h_1,\ldots,h_k \in \mathbb{F}_p^n} e_p\left((\Delta_{h_1} \cdots \Delta_{h_k} f)(0)\right) \right|.$$

High rank means f is strongly quasirandom.

Analytic Rank

The analytic rank (Gowers–Wolf, 2011) of a polynomial f of degree k is

$$r(f) = -\log_p \left| \mathbb{E}_{h_1,\ldots,h_k \in \mathbb{F}_p^n} e_p\left((\Delta_{h_1} \cdots \Delta_{h_k} f)(0)\right) \right|.$$

High rank means f is strongly quasirandom.

Example

Let q be quadratic and define the bilinear form $\beta(x, y) := (\Delta_x \Delta_y q)(0)$.

Analytic Rank

The analytic rank (Gowers–Wolf, 2011) of a polynomial f of degree k is

$$r(f) = -\log_p \left| \mathbb{E}_{h_1,\ldots,h_k \in \mathbb{F}_p^n} e_p\left((\Delta_{h_1} \cdots \Delta_{h_k} f)(0)\right) \right|.$$

High rank means f is strongly quasirandom.

Example

Let q be quadratic and define the bilinear form $\beta(x, y) := (\Delta_x \Delta_y q)(0)$.

$$\left| \frac{|V(q)|}{p^n} - \frac{1}{p} \right| = \left| \mathbb{E}_x \left(\mathbb{E}_{t \in \mathbb{F}_p} e(tq(x)) - \frac{1}{p} \right) \right| \leq \mathbb{E}_{0 \neq t \in \mathbb{F}_p} \left| \mathbb{E}_x e(tq(x)) \right|$$

Analytic Rank

The analytic rank (Gowers–Wolf, 2011) of a polynomial f of degree k is

$$r(f) = -\log_p \left| \mathbb{E}_{h_1,\ldots,h_k \in \mathbb{F}_p^n} e_p\left((\Delta_{h_1} \cdots \Delta_{h_k} f)(0) \right) \right|.$$

High rank means f is strongly quasirandom.

Example

Let q be quadratic and define the bilinear form $\beta(x,y) := (\Delta_x \Delta_y q)(0)$.

$$\left| \frac{|V(q)|}{p^n} - \frac{1}{p} \right| = \left| \mathbb{E}_x \left(\mathbb{E}_{t \in \mathbb{F}_p} e(tq(x)) - \frac{1}{p} \right) \right| \leq \mathbb{E}_{0 \neq t \in \mathbb{F}_p} \left| \mathbb{E}_x e(tq(x)) \right|$$

Since $r(tq) = r(q)$ for nonzero t, it suffices to bound

$$\begin{aligned} \left| \mathbb{E}_x e(q(x)) \right|^2 &= \mathbb{E}_{x,u} e(q(x) - q(x+u)) = \mathbb{E}_{x,u} e\left(-\beta(x,u) - q(u)\right) \\ &\leq \mathbb{E}_u \left| \mathbb{E}_x e\left(-\beta(x,u)\right) \right| = \frac{|\{u : \beta(x,u) = 0 \text{ for every } x\}|}{p^n} \end{aligned}$$

Analytic Rank

The analytic rank (Gowers–Wolf, 2011) of a polynomial f of degree k is

$$r(f) = -\log_p \left| \mathbb{E}_{h_1,\ldots,h_k \in \mathbb{F}_p^n} e_p\left((\Delta_{h_1} \cdots \Delta_{h_k} f)(0) \right) \right|.$$

High rank means f is strongly quasirandom.

Example

Let q be quadratic and define the bilinear form $\beta(x,y) := (\Delta_x \Delta_y q)(0)$.

$$\left| \frac{|V(q)|}{p^n} - \frac{1}{p} \right| = \left| \mathbb{E}_x \left(\mathbb{E}_{t \in \mathbb{F}_p} e(tq(x)) - \frac{1}{p} \right) \right| \leq \mathbb{E}_{0 \neq t \in \mathbb{F}_p} \left| \mathbb{E}_x e(tq(x)) \right|$$

Since $r(tq) = r(q)$ for nonzero t, it suffices to bound

$$\begin{aligned} \left| \mathbb{E}_x e(q(x)) \right|^2 &= \mathbb{E}_{x,u} e(q(x) - q(x+u)) = \mathbb{E}_{x,u} e\left(-\beta(x,u) - q(u)\right) \\ &\leq \mathbb{E}_u \left| \mathbb{E}_x e\left(-\beta(x,u)\right) \right| = \frac{|\{u : \beta(x,u) = 0 \text{ for every } x\}|}{p^n} \end{aligned}$$

Such u form a subspace of $\mathbb{F}_p^n$ with codimension equal to the rank r of β, so the above is at most p^{-r}. Crucially $r = r(q)$.

Subspace Decomposition

For $r > 0$, call a subspace $L \leq \mathbb{F}_p[x_1, \ldots, x_n]_{\leq k}$ r-low rank if it possesses a basis $\mathcal{B}_L$ of elements of analytic rank at most r, that is,

$$\max_{f \in \mathcal{B}_L} r(f) \leq r.$$

Subspace Decomposition

For $r > 0$, call a subspace $L \leq \mathbb{F}_p[x_1, \ldots, x_n]_{\leq k}$ r-low rank if it possesses a basis $\mathcal{B}_L$ of elements of analytic rank at most r, that is,

$$\max_{f \in \mathcal{B}_L} r(f) \leq r.$$

Call a subspace H r-high rank relative to S if

$$\min_{\substack{0 \neq f \in H \\ g \in S}} r(f+g) \geq r.$$

Subspace Decomposition

For $r > 0$, call a subspace $L \leq \mathbb{F}_p[x_1, \ldots, x_n]_{\leq k}$ r-low rank if it possesses a basis $\mathcal{B}_L$ of elements of analytic rank at most r, that is,

$$\max_{f \in \mathcal{B}_L} r(f) \leq r.$$

Call a subspace H r-high rank relative to S if

$$\min_{\substack{0 \neq f \in H \\ g \in S}} r(f+g) \geq r.$$

Lemma (Decomposition)

For any $r > 0$ and subspace S, we may decompose

$$S = H \oplus L,$$

where L is r-low rank, H is r-high rank relative to L, and L contains every r-low rank subspace in S. Then $V(S) = V(H) \cap V(L)$.

Quasirandom estimate

Lemma (Relative density)

Let H be r-high rank relative to L. Set $h := \dim(H)$. Then

$$\left| \frac{|V(H) \cap V(L)|}{|V(L)|} - p^{-h} \right| \leq \frac{p^{n-r/2^{k-1}}}{|V(L)|}.$$

Quasirandom estimate

Lemma (Relative density)

Let H be r-high rank relative to L. Set $h := \dim(H)$. Then

$$\left| \frac{|V(H) \cap V(L)|}{|V(L)|} - p^{-h} \right| \leq \frac{p^{n - r/2^{k-1}}}{|V(L)|}.$$

Proof sketch: For $x \in \mathbb{F}_p^n$ write $1_{x \in V(H \oplus L)} = \mathbb{E}_{f \in H \oplus L} e_p(f(x))$ and then use the exponential sum bound

$$\left| \mathbb{E}_{x \in \mathbb{F}_p^n} e_p(f(x)) \right| \leq p^{-r(f)/2^{k-1}}.$$



Low rank subspaces

Lemma (Low rank count)

For $k < p < r$ there are at most $p^{O_k(n^{k-1} r \log_p r)}$ polynomials $\mathbb{F}_p^n \to \mathbb{F}_p$ with degree at most k and analytic rank at most r.

Low rank subspaces

Lemma (Low rank count)

For $k < p < r$ there are at most $p^{O_k(n^{k-1} r \log_p r)}$ polynomials $\mathbb{F}_p^n \to \mathbb{F}_p$ with degree at most k and analytic rank at most r.

Allows us to union bound over the number of low rank subspaces of a given dimension.

Low rank subspaces

Lemma (Low rank count)

For $k < p < r$ there are at most $p^{O_k(n^{k-1} r \log_p r)}$ polynomials $\mathbb{F}_p^n \to \mathbb{F}_p$ with degree at most k and analytic rank at most r.

Allows us to union bound over the number of low rank subspaces of a given dimension.

Lemma (Warning's second theorem)

Let S be a subspace with dimension s. If $|V(S)| \geq 1$ then

$$|V(S)| \geq p^{n-sk}.$$

Furthermore, this is tight.

Low rank subspaces

Lemma (Low rank count)

For $k < p < r$ there are at most $p^{O_k(n^{k-1} r \log_p r)}$ polynomials $\mathbb{F}_p^n \to \mathbb{F}_p$ with degree at most k and analytic rank at most r.

Allows us to union bound over the number of low rank subspaces of a given dimension.

Lemma (Warning's second theorem)

Let S be a subspace with dimension s. If $|V(S)| \geq 1$ then

$$|V(S)| \geq p^{n-sk}.$$

Furthermore, this is tight.

Tells us exactly the smallest density α we need to consider in the relative threshold result.

[]

Relative threshold

Lemma

Fix an r-low rank subspace L with dimension ℓ. Let $\alpha := |V(L)| \cdot p^{-n}$. Let $\mathcal{H}_{k,h,L}$ be the collection of varieties generated by subspaces $S = H \oplus L$ where H is r-high rank relative to L with dimension $h > 0$. Then letting

$$t_h := \frac{\log(p^h)}{\log(1 + (p^h - 1)^{-1})},$$

we have for every $\varepsilon \in (0, 1)$ that if $|M| \geq (\alpha^{-1} t_h + \varepsilon)\binom{n}{k}$ then

$$\mathbb{P}\left(M \text{ pierces } \mathcal{H}_{k,h,L}\right) \geq 1 - 2\exp\left(-\frac{(\alpha\varepsilon)^2}{8(t_h + \alpha\varepsilon)}\binom{n}{k}\right),$$

and if $|M| \leq (\alpha^{-1} t_h - \varepsilon)\binom{n}{k}$ then

$$\mathbb{P}\left(M \text{ pierces } \mathcal{H}_{k,h,L}\right) = o(1)$$

as $n \to \infty$.

Threshold for fixed rank parameters

Lemma

Let $\mathcal{I}_{k,h,\ell}$ be the collection of nonempty varieties generated by subspaces $S = H \oplus L$ with $\dim(L) = \ell, \dim(H) = h > 0$ and such that H is r-high rank relative to L. Then letting

$$d_{h,\ell} := p^{\ell k} \cdot t_h = p^{\ell k} \cdot \frac{\log(p^h)}{\log(1 + (p^h - 1)^{-1})},$$

we have for every $\varepsilon > 0$

$$\mathbb{P}(M \text{ pierces } \mathcal{I}_{k,h,\ell}) = \begin{cases} 1 - o(1), & |M| \geq (d_{h,\ell} + \varepsilon)\binom{n}{k} \\ o(1), & |M| \leq (d_{h,\ell} - \varepsilon)\binom{n}{k} \end{cases},$$

as $n \to \infty$.

Full threshold now follows by union bound and noting that $c_{k,s} = d_{1,s-1}$ maximizes the above threshold.