RANDOM SYMMETRIC MATRICES

Letícia Mattos
IMPA

Joint work with M. Campos, R. Morris and N. Morrison

Invertibility of Random Matrices

Let A_n be a random $n \times n$ matrix with entries in $\{-1, 1\}$.

Invertibility of Random Matrices

Let A_n be a random $n \times n$ matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(A_n) = 0]$?

Invertibility of Random Matrices

Let A_n be a random $n \times n$ matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(A_n) = 0]$?

Lower bound:

$$\mathbb{P}[\det(A_n) = 0] \geq \mathbb{P}[\exists \text{ rows } r_i, r_j \text{ s.t. } r_i = \pm r_j]$$

Invertibility of Random Matrices

Let A_n be a random $n \times n$ matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(A_n) = 0]$?

Lower bound:

$$\mathbb{P}[\det(A_n) = 0] \geq \mathbb{P}[\exists \text{ rows } r_i, r_j \text{ s.t. } r_i = \pm r_j]$$

$$\geq (1 + o(1)) \, n^2 \, 2^{-n}$$

Invertibility of Random Matrices

Let A_n be a random $n \times n$ matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(A_n) = 0]$?

Lower bound:

$$\mathbb{P}[\det(A_n) = 0] \geq (1 + o(1)) n^2 2^{-n+1}$$

Invertibility of Random Matrices

Conjecture (Folklore):

$$\mathbb{P}[\det(A_n) = 0] = (1 + o(1))\, n^2\, 2^{-n+1}$$

Invertibility of Random Matrices

Conjecture (Folklore):

$$\mathbb{P}[\det(A_n) = 0] = (1 + o(1))\, n^2\, 2^{-n+1}$$

Upper bounds on $\mathbb{P}[\det(A_n) = 0]$:

Invertibility of Random Matrices

Conjecture (Folklore):

$$\mathbb{P}[\det(A_n) = 0] = (1 + o(1))\, n^2\, 2^{-n+1}$$

Upper bounds on $\mathbb{P}[\det(A_n) = 0]$:

Komlós '67 : $O(n^{-1/2})$

Kahn, Komlós, Szemerédi '95 : $(1-\varepsilon)^n$

Tao, Vu '07 : $(3/4 + o(1))^n$

Bourgain, Vu, Wood '10 : $\left(\frac{1}{\sqrt{2}} + o(1)\right)^n$

Tikhomirov '18 : $\left(\frac{1}{2} + o(1)\right)^n$

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(M_n) = 0]$?

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Question: What is $\mathbb{P}[\det(M_n) = 0]$?

Natural conjecture: $\mathbb{P}[\det(M_n) = 0] = \Theta(n^2 2^{-n})$

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Upper bounds on $\mathbb{P}[\det(M_n) = 0]$:

Costello, Tao, Vu '05 : $n^{-1/8 + o(1)}$

Nguyen '12 : $O(n^{-c})$, for any $c > 0$

Vershynin '14 : $\exp(-n^c)$

Ferber, Jain '18 : $\exp(-c\, n^{1/4} \log n)$

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Theorem (Campos, M., Morris, Morrison '19$^+$)

$\exists\, c > 0$ such that

$$\mathbb{P}[\det(M_n) = 0] \leq \exp(-c\sqrt{n})$$

Invertibility of SYMMETRIC Random Matrices

Let M_n be a random $n \times n$ symmetric matrix with entries in $\{-1, 1\}$.

Theorem (Campos, M., Morris, Morrison '19$^+$)

$\exists\, c > 0$ such that

$$\mathbb{P}[\det(M_n) = 0] \leq \exp(-c\sqrt{n})$$

Key Ingredient: Inverse Littlewood-Offord theorem inspired by containers

The Littlewood-Offord Problem

The Littlewood-Offord Problem

For any abelian group G, $n \in \mathbb{N}$ and $v \in G^n$, define

$$\rho(v) := \max_{a \in G} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a]$$

where $x \sim U(\{-1,1\}^n)$.

The Littlewood-Offord Problem

For any abelian group G, $n \in \mathbb{N}$ and $v \in G^n$, define

$$\rho(v) := \max_{a \in G} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a]$$

where $x \sim U(\{-1,1\}^n)$.

In our case, G will be either $\mathbb{Z}$ or $\mathbb{Z}_p$, for p prime.

The Littlewood-Offord Problem

For any abelian group G, $n \in \mathbb{N}$ and $v \in G^n$, define

$$\rho(v) := \max_{a \in G} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a]$$

where $x \sim U(\{-1,1\}^n)$.

In our case, G will be either $\mathbb{Z}$ or $\mathbb{Z}_p$, for p prime.

Question: what upper bounds on $\rho(v)$ can be proven?

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

Theorem (Erdős '45) $\rho(v) \leq \dfrac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O\left(\dfrac{1}{\sqrt{n}}\right)$

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

Theorem (Erdős '45) $\rho(v) \leq \dfrac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O\left(\dfrac{1}{\sqrt{n}}\right)$

This is best possible! (take $v_i = 1 \ \forall i$)

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

Theorem (Erdős '45) $\rho(v) \leq \dfrac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O\left(\dfrac{1}{\sqrt{n}}\right)$

This is best possible! (take $v_i = 1 \ \forall i$)

Question (Tao, Vu): $\rho(v)$ is large $\Rightarrow$ v has structure?

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

Theorem (Erdős '45) $\rho(v) \leq \dfrac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O\left(\dfrac{1}{\sqrt{n}}\right)$

This is best possible! (take $v_i = 1 \ \forall i$)

Question (Tao, Vu): $\rho(v)$ is large $\Rightarrow$ v has structure?

$\rho(v) \geq n^{-c} \Rightarrow$ At least $\dfrac{2^n}{n^c}$ sums are equal!

The Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n).$$

Theorem (Erdős '45) $\rho(v) \leq \dfrac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O\left(\dfrac{1}{\sqrt{n}}\right)$

This is best possible! (take $v_i = 1 \ \forall i$)

Question (Tao, Vu): $\rho(v)$ is large $\Rightarrow$ v has structure?

$\rho(v) \geq n^{-c} \Rightarrow$ At least $\dfrac{2^n}{n^c}$ sums are equal!

$\Rightarrow$ v must have some arithmetic structure!

The INVERSE Littlewood-Offord Problem

In fact, it was shown by Tao, Vu and Nguyen, Vu that if $\rho(v) \geq n^{-c}$ then $v \subset Q$, for some 'small' generalised arithmetic progression Q...

The INVERSE Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}_p} \mathbb{P}\left[x_1 v_1 + \cdots + x_n v_n = a \right], \quad x \sim U\left(\{-1,1\}^n\right)$$

The INVERSE Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}_p} \mathbb{P}[x_1 v_1 + \cdots + x_n v_n = a], \quad x \sim U(\{-1,1\}^n)$$

If $\rho(v) \geq \frac{4}{p}$ we can also say something about the structure of v!

The INVERSE Littlewood-Offord Problem

$$\rho(v) := \max_{a \in \mathbb{Z}_p} \mathbb{P}\left[x_1 v_1 + \cdots + x_n v_n = a \right], \quad x \sim U\left(\{-1,1\}^n\right)$$

Theorem (Campos, M., Morris, Morrison '19$^+$)

Let p be prime. There exists a family $\mathcal{C}$ of subsets of $\mathbb{Z}_p$, with $|\mathcal{C}| \leq \exp\left(2^{12} (\log p)^2\right)$, such that $\forall\, n \in \mathbb{N}$, $v \in \mathbb{Z}_p^n$ with $\rho(v) \geq \frac{4}{p}$ and $|v| \geq 2^{18} \log p$, $\exists\, B(v) \in \mathcal{C}$ such that

$$|B(v)| \leq \frac{2^{16}}{\rho(v)\sqrt{|v|}} \quad \text{and} \quad \#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$$

But... WAIT!!!

WHAT DOES THIS HAVE TO DO WITH RANDOM MATRICES?

Reducing the problem:

Reducing the problem:

The problem reduces to bounding

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega,\ \rho(v) \geq \beta\right]$$

Reducing the problem:

The problem reduces to bounding

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega,\ \rho(v) \geq \beta\right]$$

Think of $\beta \sim \exp(-c\sqrt{n})$ and $p \sim \frac{1}{\beta}$

Reducing the problem:

The problem reduces to bounding

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right]$$

Think of $\beta \sim \exp(-c\sqrt{n})$ and $p \sim \frac{1}{\beta}$

We 'essentially' have:

Lemma (Ferber, Jain) $\mathbb{P}[\det(M_n) = 0] \leq n^2 \left(\beta + \frac{q_n(\beta)}{\beta}\right)$

Reducing the problem:

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega,\ \rho(v) \geq \beta\right]$$

Reducing the problem:

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right]$$

Theorem (Campos, M., Morris, Morrison '19$^+$)

For $p \leq \exp(c\sqrt{n})$ prime and $\beta \geq \frac{4}{p}$,

$$q_n(\beta) \leq 2^{-n/4}$$

Reducing the problem:

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega,\ \rho(v) \geq \beta\right]$$

Theorem (Campos, M., Morris, Morrison '19+)

For $p \leq \exp(c\sqrt{n})$ prime and $\beta \geq \frac{4}{p}$,

$$q_n(\beta) \leq 2^{-n/4}$$

It follows that $n^2\left(\beta + \frac{q_n(\beta)}{\beta}\right) \leq \exp(-c\sqrt{n})$

for $\beta = \frac{4}{p}$ and $p \sim \exp(c\sqrt{n})$

Reducing the problem:

$$q_n(\beta) := \max_{\omega \in \mathbb{Z}_p^n} \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right]$$

Theorem (Campos, M., Morris, Morrison '19+)

For $p \leq \exp(c\sqrt{n})$ prime and $\beta \geq \frac{4}{p}$,

$$q_n(\beta) \leq 2^{-n/4}$$

It follows that $n^2\left(\beta + \frac{q_n(\beta)}{\beta}\right) \leq \exp(-c\sqrt{n})$

for $\beta = \frac{4}{p}$ and $p \sim \exp(c\sqrt{n}) \Rightarrow \mathbb{P}[\det = 0] \leq \exp(-c\sqrt{n})$

How to bound

$$q_n(\beta, \omega) := \mathbb{P}\left[\exists\, v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega,\ \rho(v) \geq \beta\right] ?$$

How to bound

$$q_n(\beta, \omega) := \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right] ?$$

Union bound doesn't work!

How to bound

$$q_n(\beta, w) := \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = w, \rho(v) \geq \beta\right] ?$$

Union bound doesn't work!

$|\mathbb{Z}_p^n| = p^n$ and $\mathbb{P}[Mv = w] \leq 2^{-n}$ but

$$p^n 2^{-n} \longrightarrow \infty$$

How to bound

$$q_n(\beta, \omega) := \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right] ?$$

Union bound doesn't work!

$|\mathbb{Z}_p^n| = p^n$ and $\mathbb{P}[Mv = \omega] \leq 2^{-n}$ but

$$p^n 2^{-n} \longrightarrow \infty$$

But we don't have that many vectors!

How to bound

$$q_n(\beta, \omega) := \mathbb{P}\left[\exists v \in \mathbb{Z}_p^n \setminus \{0\} : M_n v = \omega, \rho(v) \geq \beta\right] ?$$

Union bound doesn't work!

$|\mathbb{Z}_p^n| = p^n$ and $\mathbb{P}[Mv = \omega] \leq 2^{-n}$ but

$$p^n 2^{-n} \longrightarrow \infty$$

But we don't have that many vectors!

$\rho(v) \geq 2^{-\sqrt{n}} \Rightarrow$ v is structured and there are very 'few' of them!

Remember our inverse Littlewood-Offord thm:

$\exists\ \mathcal{C} \subset 2^{\mathbb{Z}^n}$, $|\mathcal{C}| \leq \exp(2^{-8}n)$ s.t.

if $\rho(v) \geq \frac{4}{2^{\sqrt{n}}}$ and $|v| \geq \sqrt{n}$ then $\exists\ B(v) \in \mathcal{C}$ s.t.

$|B(v)| \leq \frac{1}{\rho(v)\sqrt{n}}$ and $\#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$

Remember our inverse Littlewood-Offord thm:

$\exists\ \mathcal{C} \subset 2^{\mathbb{Z}^n}$, $|\mathcal{C}| \leq \exp(2^{-8}n)$ s.t.

if $\rho(v) \geq \frac{4}{2^{\sqrt{n}}}$ and $|v| \geq \sqrt{n}$ then $\exists\ B(v) \in \mathcal{C}$ s.t.

$|B(v)| \leq \frac{1}{\rho(v)\sqrt{n}}$ and $\#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$

Let us do union bound using these containers:

Remember our inverse Littlewood-Offord thm:

$\exists\ \mathcal{C} \subset 2^{\mathbb{Z}^n}$, $|\mathcal{C}| \leq \exp(2^{-8}n)$ st

if $\rho(v) \geq \frac{4}{2^{\sqrt{n}}}$ and $|v| \geq \sqrt{n}$ then $\exists\ B(v) \in \mathcal{C}$ st

$|B(v)| \leq \frac{1}{\rho(v)\sqrt{n}}$ and $\#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$

Let us do union bound using these containers:

$$q_n(p,\omega) \leq \sum_{B \in \mathcal{C}} \mathbb{P}[\exists v \text{ st } v \subset B, \rho(v) \geq \tfrac{4}{p} \text{ and } Mv = \omega] + 2^{-cn}$$

Remember our inverse Littlewood-Offord thm:

$\exists\ \mathcal{C} \subset 2^{\mathbb{Z}^n}$, $|\mathcal{C}| \leq \exp(2^{-8}n)$ st

if $\rho(v) \geq \frac{4}{2^{\sqrt{n}}}$ and $|v| \geq \sqrt{n}$ then $\exists\ B(v) \in \mathcal{C}$ st

$$|B(v)| \leq \frac{1}{\rho(v)\sqrt{n}} \quad \text{and} \quad \#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$$

Let us do union bound using these containers:

$$q_n(\beta, \omega) \leq \sum_{B \in \mathcal{C}} \mathbb{P}\left[\exists v \text{ st } v \subset B, \rho(v) \geq \tfrac{4}{\beta} \text{ and } Mv = \omega\right] + 2^{-cn}$$

comes from vectors of small support

Remember our inverse Littlewood-Offord thm:

$\exists\ \mathcal{C} \subset 2^{\mathbb{Z}^n}$, $|\mathcal{C}| \leq \exp(2^{-8}n)$ st

if $\rho(v) \geq \frac{4}{2^{\sqrt{n}}}$ and $|v| \geq \sqrt{n}$ then $\exists\ B(v) \in \mathcal{C}$ st

$$|B(v)| \leq \frac{1}{\rho(v)\sqrt{n}} \quad \text{and} \quad \#\{i \in [n] : v_i \notin B(v)\} \leq \frac{n}{4}$$

Let us do union bound using these containers:

$$q_n(p,\omega) \leq \sum_{B \in \mathcal{C}} \underbrace{\mathbb{P}[\exists\, v \text{ st } v \subset B,\ \rho(v) \geq \tfrac{4}{p} \text{ and } Mv = \omega]}_{(*)} + 2^{-cn}$$

comes from vectors of small support

Because $\rho(v) \leqslant \frac{c}{|B(v)|\sqrt{n}}$, it follows that

Because $\rho(v) \leq \frac{c}{|B(v)|\sqrt{n}}$, it follows that

(*) $\mathbb{P}\left[\exists\, v \text{ s.t. } v \subset B,\ \rho(v) \geq \frac{q}{p} \text{ and } Mv = w\right] \leq \sum_{v \in B^n} \mathbb{P}\left[Mv = w\right]$

Because $\rho(v) \leq \frac{c}{|B(v)|\sqrt{n}}$, it follows that

$$(*)\quad \mathbb{P}\left[\exists\, v \text{ s.t. } v \subset B,\ \rho(v) \geq \tfrac{q}{p} \text{ and } Mv = w\right] \leq \sum_{v \in B^n} \mathbb{P}\left[Mv = w\right]$$

$$\leq \sum_{v \in B^n} \left(\frac{c}{|B|\sqrt{n}}\right)^n$$

Because $\rho(v) \leqslant \frac{c}{|B(v)|\sqrt{n}}$, it follows that

$$(*)\quad \mathbb{P}\left[\exists\, v \text{ st } v \subset B,\ \rho(v) \geqslant \tfrac{q}{p} \text{ and } Mv = w\right] \leqslant \sum_{v \in B^n} \mathbb{P}\left[Mv = w\right]$$

$$\leqslant \sum_{v \in B^n} \left(\frac{c}{|B|\sqrt{n}}\right)^n$$

$$\leqslant \exp\left(-\tfrac{1}{4} n \log n\right)$$

Because $\rho(v) \leqslant \frac{c}{|B(v)|\sqrt{n}}$, it follows that

$$(*)\quad \mathbb{P}\left[\exists\, v \text{ st } v \subset B,\ \rho(v) \geqslant \tfrac{q}{p} \text{ and } Mv = w\right] \leqslant \sum_{v \in B^n} \mathbb{P}\left[Mv = w\right]$$

$$\leqslant \sum_{v \in B^n} \left(\frac{c}{|B|\sqrt{n}}\right)^n$$

$$\leqslant \exp\left(-\tfrac{1}{4} n \log n\right)$$

Because we have $< \exp\left(2^{-8} n \log n\right)$ elements on $\mathcal{C}$, we get

Because $\rho(v) \leqslant \frac{c}{|B(v)|\sqrt{n}}$, it follows that

$$(*)\quad \mathbb{P}\left[\exists v \text{ st } v \subset B,\ \rho(v) \geqslant \tfrac{q}{p} \text{ and } Mv = w\right] \leqslant \sum_{v \in B^n} \mathbb{P}\left[Mv = w\right]$$

$$\leqslant \sum_{v \in B^n} \left(\frac{c}{|B|\sqrt{n}}\right)^n$$

$$\leqslant \exp\left(-\tfrac{1}{4} n \log n\right)$$

Because we have $< \exp\left(2^{-8} n \log n\right)$ elements on $\mathcal{C}$, we get

$$q_n(p, w) \leqslant \sum_{B \in \mathcal{C}} \exp\left(-\tfrac{1}{4} n \log n\right) + 2^{-cn} \leqslant 2^{-cn}$$

:)

Thank you!