Singularity of random ±1 matrices

We prove the following result of Kahn, Komlós, Szemerédi:

Let M_n be $n \times n$ ± 1 matrix where

$$\Pr(M_n(i,j) = 1) = 1/2 \quad \forall i, j. \text{ (independently)}$$

Then $\exists$ constant $c < 1$ such that

$$\Pr(M_n \text{ is singular}) \leq c^n.$$

Tao, Vu reduced c to $3/4$

$c = \frac{1}{2} + o(1)$ is best possible.

$$M_n = [X_1, X_2, \ldots, X_n]$$

columns

<u>Proposition</u>

Let Ω_1 be the set of $v \in \mathbb{Z}^n$ with at least $3n/\log_2 n$ zero coordinates. Then

$$\Pr(\underbrace{\exists v \in \Omega_1 : M_n v = 0}_{\mathcal{E}}) \le (1+o(1)) n^2 2^{-n}$$

<u>Proof</u>

$$\Pr(\mathcal{E}) = \sum_{2 \le k \le n - 3n/\log_2 n} \Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \quad \text{where}$$

$$= \{\exists v = (a_1, \ldots, a_n) : k \text{ of } a_i \text{ are non-zero}, \ a_1X_1 + \cdots + a_nX_n = 0\}$$

$$\Pr(\mathcal{E}_2) \le \mathbb{E}[\#\text{pairs } X_i = \pm X_j] \le n^2 2^{-n}.$$

Assume $k \ge 3$.

$$\Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \le \binom{n}{k} \Pr(\underbrace{\mathcal{F}_k}_{\left\{\begin{array}{l}\exists\ a_1 X_1 + \cdots + a_k X_k = 0 \\ \quad a_1, \ldots, a_k \ne 0\end{array}\right\}} \setminus \mathcal{E}_{k-1})$$

$\mathcal{F}_k \setminus \mathcal{E}_{k-1} \Rightarrow$ matrix $A_k = [X_1, X_2, \ldots, X_k]$

has rank $k-1$.

Hence $\exists$ $k-1$ rows R of A_k that "determine"

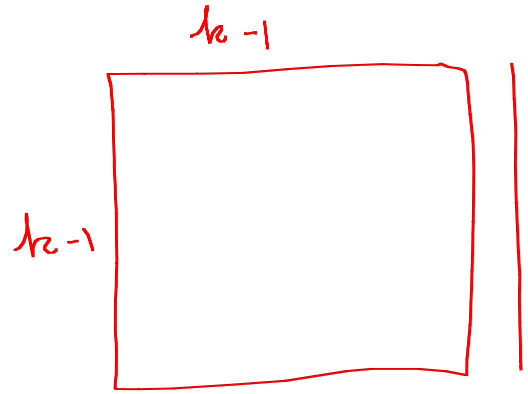
$a_1, \ldots, a_k$ (up to scaling).

$$\Pr(\mathcal{E}_k / \mathcal{E}_{k-1})$$

$$\sum_{M_n(R,C)}$$

$$\leq \sum_{C} \sum_{R} \Pr\left(\mathcal{F}_k \setminus \mathcal{E}_{k-1} \mid M_n(R,C)\right) \Pr\left(M_n(R,C)\right)$$

C: k cols   R: k-1 rows



remaining $n-k+1$ rows here to behave.

$a_1, \dots, a_k$ fixed up to scaling

$$\leq \binom{n}{k}\binom{n}{k-1} \rho^{n-k+1} \overbrace{\sum_{M_n(\square)} \Pr\left(M_n(\square)\right)}^{1}$$

where ρ is an upper bound on $\Pr[a_1 Z_1 + \dots + a_k Z_k = 0]$ for $a_1, \dots, a_k \in \mathbb{Z} \setminus \{0\}$, $Z_i = \pm 1$ independently.

We argue later that

$$\rho \leq \binom{k}{\lfloor k/2 \rfloor} 2^{-k} \leq \frac{1}{\sqrt{k}} \qquad \circledast$$

Thus

$$\sum_{3 \leq k \leq n - 3n/\log_2 n} \Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \leq \sum_{3 \leq k \leq \cdots} \binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1}$$

(i) $k \leq \epsilon n$: $\binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1} \leq e^{O(\epsilon \ln 1/\epsilon \; n)} \cdot \left(\frac{1}{\sqrt{3}}\right)^{(1-\epsilon)n}$

(ii) $\epsilon n < k \leq n - \frac{3n}{\log_2 n}$: $\binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1}$

$$\leq 2^n \times 2^n \times \left(\frac{1}{\sqrt{\epsilon n}}\right)^{3n/\log_2 n} \longleftarrow \text{take logs}$$

Proof of ⊛ : Littlewood-Offord Problem.

$$\mathcal{A} \subseteq 2^{[n]} \text{ \& } A, B \subseteq \mathcal{A} \ni A \nsubseteq B$$

then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Erdös: Suppose $a_1, a_2, \ldots, a_n \in \mathbb{R}_+$ with $|a_i| \geq 1$.

Let I be any open interval of width 2.

$$\left|\{(z_1, z_2, \ldots, z_n) \in \{-1, 1\}^n : a_1 z_1 + \cdots + a_n z_n \in I\}\right| \leq \binom{n}{\lfloor \frac{1}{2} n \rfloor}.$$

We can assume w.l.o.g. that $a_1, \ldots, a_n \geq 1$ $[a_i \to -a_i$ is ok$]$

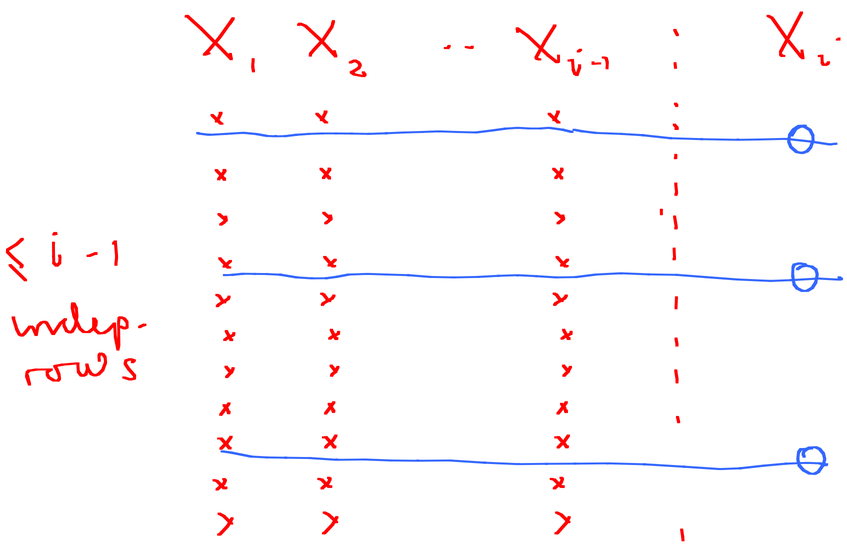
$\mathcal{A} = \{A : Z_A = \sum_{i \in A} a_i - \sum_{i \notin A} a_i \in I\}$ is a Sperner family

$(A \subsetneq B \Rightarrow Z_B \geq Z_A + 2\})$.

Proposition

$$\Pr\left(X_i \in \operatorname{span}(X_1, X_2, \ldots, X_{i-1})\right) \leq \min\left\{2^{i-n-1}, O(1/\sqrt{n})\right\}$$

Proof



condition on rows and values of $X_1, \ldots, X_i$ in these $i-1$ rows.

Remaining entries of X_i are determined and $\Pr \leq \frac{1}{2}$ that they are chosen.

This gives upper bound of 2^{i-n-1}.

Now assume that $i \geq .9n$.

Choose a hyperplane $H: \{a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0\}$

that contains $X_1, X_2, \ldots, X_i$.

We can assume by Proposition P2 that

$\Omega(n)$ of the a_i are non-zero.

But then

$$\Pr(X_i \in H) = O(1/\sqrt{n}).$$

$\square$

Thus for some $c > 0$

$$\Pr(M_n \text{ is singular}) \le \sum_{i=2}^{n} \min\left\{2^{i-n-1}, \frac{c}{\sqrt{n}}\right\}$$

$$= \sum_{i=2}^{n-\frac{1}{2}\log_2 n} 2^{i-n-1} + \sum_{i=n-\frac{1}{2}\log_2 n}^{n} \frac{c}{\sqrt{n}}$$

$$= O\left(\frac{\log n}{\sqrt{n}}\right).$$

$\square$

We continue with a proof of an exponential upper bound.

Now let

$$\Omega_2 = \{ v \in \mathbb{Z}^n : |v_i| \le n^C, \forall i \}$$

Here C is some constant.

Proposition

$$\Pr(\exists v \in \Omega_2 : M_n v = 0) \le \left(\tfrac{1}{2} + o(1)\right)^n.$$

Proof

For $v \in \Omega_2$, let $p(v) = \Pr(X \cdot v = 0)$ when $X \overset{\text{ran}}{\in} \{\pm 1\}^n$

(I) $\Pr(M_n v = 0) = p(v)^n$

(II) $p(v) \le 1/2$: $\Pr(X \cdot v = 0) = \Pr(X_1 v_1 = -\sum_{j=2}^{n} X_j v_j) \le \frac{1}{2}$

assuming $v_1 \ne 0$.

Let $S_j = |\{v \in \Omega_2 : 2^{-j-1} \le p(v) \le 2^{-j}\}|$

$$\Pr(\exists v \in \Omega_2 : M_n v = 0) \le \sum_{j=1}^{n} (2^{-j})^n S_j$$

[Note $p(v) = 0$ or $p(v) \ge \frac{1}{2^n}$ — there are 2^n choices for X]

If $p(v) \geq n^{-1/3}$ then $\binom{k}{\lfloor k/2 \rfloor} 2^{-k} \geq n^{-1/3}$

Littlewood - Offord - Erdős

where $k = |\{ j : v_j \neq 0 \}|$.

& thus $k = O(n^{2/3})$ and $v \in \Omega_1$.

$|\Omega_2| \leq n^{(C+1)n}$ and so $\sum_{2^{-j} \leq n^{-C-2}} (2^{-j})^n S_j \leq 2^{-n}$.

Remains to consider

$$\sum_{n^{-C-2} \leq 2^{-j} \leq n^{-1/3}} (2^{-j})^n S_j.$$

Fix ϵ small.

Fix i and integer $d = d(i, \epsilon)$ such that

$$n^{-\frac{1}{3} - (d-1)\epsilon} > 2^{-i} \geq n^{-\frac{1}{3} - d\epsilon}$$

Now choose k such that

$$k^{d-1} \ll n^{\frac{1}{3} + (d-1)\epsilon} \qquad (a)$$

$$k^{d} \gg n^{\frac{1}{3} + d\epsilon} \qquad (b)$$

$$k = n^{\frac{1}{3(d - 1/2)} + \epsilon}$$

Proposition

G is torsion free or of odd order.

For any $d \geq 1$ there is a constant δ_d such that the following holds: suppose $k \geq 2$ and $x \in G$ and $v \in G^n$. Then either

(i) $\Pr(x_1 v_1 + x_2 v_2 + \cdots + x_n v_n = x) \leq \delta_d k^{-d}$

$x_i = \pm 1$ random only

or

(ii) $\exists\, P = [-k, k]^{d-1} \cdot (w_1, \ldots, w_{d-1}) \subseteq G$

and $a_j \in [k]$ such that $a_j v_j \in P$ for all but at most k^2 exceptional values.

Furthermore $w_1, \ldots, w_{d-1} \in \{v_1, \ldots, v_n\}$.

It follows from (b) on P13 that condition 1 fails.

Assume condition 2 and estimate S_j.

$S_j \leq$ # choices for P $\times$ # choices for exceptional value

$(2n^c+1)^{d-1}$ $\qquad \leq \binom{n}{k^2}(2n^c+1)^{k^2}$

$\times$ choices for rest of v_i

$(|P|\, n)^{o(n)}$

(i) a_j is a factor of some $x \in P$

(ii) Integer N has $\leq N^{o(1)}$ factors

Hence
$$S_j \leq n^{O(k^2)}\, O(1)^n\, k^{(d-i+o(1))n}$$

and then

$$(2^{-j})^n S_j \leq O(1)^n \left[n^{\frac{d-1}{d-\frac{1}{2}}\cdot\frac{1}{3}+(d-1)\epsilon+o(1)-\frac{1}{3}-(d-1)\epsilon} \right]^n$$

$$= O(1)^n\, n^{-n\epsilon/6d-3}$$

$\#j = O(\log n)$ $\qquad \square$

Proposition

$$\Pr[M_n \text{ is singular}] = 2^{O(n)} \Pr[\dim(X_1, \dots, X_n) = n-1]$$

Proof

$$\Pr[M_n \text{ is singular}] \geq \Pr[\dim(X_1, \dots, X_n) = n-1].$$

On the other hand: if $X_1, \dots, X_n$ are dependent then $\exists\, d$ such that $X_1, \dots, X_d$ are independent and $X_{d+1} \in \mathrm{Span}(X_1, \dots, X_d)$. Denote this event by $\mathcal{E}_d$.

$$\Pr[\dim(X_1, \dots, X_n) = n-1 \mid \mathcal{E}_d] \geq \prod_{j \geq d+1} \left(1 - \min\left\{\frac{1}{2^{n-d+1}}, \frac{c}{\sqrt{n}}\right\}\right)$$

$$= 2^{-O(n)}.$$

[Just modify proof Prop 7. Here one can fix $X_1, \dots, X_{i-1}$ and $i-1$ coordinates of X_i]

So

$$\underbrace{\sum_d \Pr\left(\dim(X_1,\dots,X_n) = n-1 \wedge \mathcal{E}_j\right)}_{\Pr(\dim(X_1,\dots,X_n)=n-1)} \geq 2^{-O(n)} \underbrace{\sum_d \Pr(\mathcal{E}_d)}_{\Pr(M_n \text{ is singular})}$$

Suffices to show that

$$\sum_V \Pr(X_1,\dots,X_n \text{ span } V) \leq (1-\epsilon_1)^n$$

Sum over V: V is spanned by $n-1$ independent vectors in $\{\pm 1\}^n$.

Density of V: $\Pr(X \in V) = \dfrac{|V \cap \{-1,1\}^n|}{2^n}$

<u>Proposition</u>

$$\Omega_\alpha = \{ V : \Pr[X \in V] \leq \alpha \}$$

$$\sum_{V \in \Omega_\alpha} \Pr(\operatorname{span}(X) = V) \leq n\alpha$$

<u>Proof</u>

$$\sum_{V \in \Omega_\alpha} \Pr(\operatorname{span}(X) = V) = \sum_{i} \sum_{X_{\neq i}} \Pr[X_{\neq i}] \underbrace{\Pr[X_i \in \overbrace{\operatorname{span}(X_{\neq i})}^{V}]}_{\leq \alpha}$$

$$\left(\tfrac{1}{2}\right)^{n(n-1)}$$

$$\leq \alpha \sum_i \underbrace{\left[\sum_{X_{\neq i}} \Pr[X_{\neq i}] \right]}_{1} \leq n\alpha$$

$\square$

From Propositions 16 and 18 we can finish by estimating

$$\Pr\left[V = \mathrm{span}(X_1, \dots, X_n) \text{ is an } (n-1) \text{ dimensional hyperplane and } (1-\epsilon_1)^n \leq \Pr[X \in V] \leq \frac{C}{\sqrt{n}} \right]$$

Here C is a large enough constant so that if $\Pr[X \in V] \geq \frac{C}{\sqrt{n}}$ then at most $c'n$ coefficients of the equation defining V are non-zero, where $c' < 1$ is constant.

Fix $v = (v_1, v_2, \dots, v_n)$ and $0 \leq \mu \leq 1$

$$X_v^{(\mu)} = \sum_{i=1}^{n} \eta_i^{(\mu)} v_i \quad \text{where} \quad \eta_i^{(\mu)} = \begin{cases} 0 & \text{Prob } 1-\mu \\ -1 & \text{Prob } \mu/2 \\ +1 & \text{Prob } \mu/2 \end{cases}$$

Proposition

Let G be torsion free or cyclic of odd prime order. Let $v \in G^n$ and $0 < \mu \leq \mu' \leq 1$ with $\mu \leq 1/4$. Then

$$\Pr[X_v^{(\mu')} = x] = O\left(\sqrt{\frac{\mu}{\mu'}} \Pr(X_v^{(\mu)} = 0)\right) + O\left(\Pr(X_v^{(\mu)} = 0)^{\Omega(\mu'/\mu)}\right)$$

Suppose $0 < \mu \ll 1$ and $Y \in \{0, \pm 1\}^n = (\eta_1^{(\mu)}, \dots, \eta_n^{(\mu)})$.

Taking $\mu' = 1$ in Proposition 20 and μ small enough

$$\Pr[X \in V] = O(\sqrt{\mu}) \Pr(Y \in V). \qquad \circledast$$

Here $X_v^{(\mu')} = X \cdot v$ and $X_v^{(\mu)} = Y \cdot v$

Also we can assume $\Pr(Y \in V) = O(1/\sqrt{n})$: whp $\Omega(n)$ of the Y_i are non-zero. Apply L.O.

Choose small δ and a density σ such that $(1-\epsilon_1)^n \leq \sigma \leq c/\sqrt{n}$ and let V be such that $\Pr(X \in V) = (1 + O(1/n))\, \sigma$.

Now choose $Y_1, Y_2, \dots Y_{\delta n}$ independently of $X_1, X_2, \dots, X_n$.

$$(*) \quad \Pr(Y_1, \dots, Y_{\delta n} \in V) \geq \Omega(1/\sqrt{\mu})^{\delta n} \sigma^{\delta n}$$

$(*)$ on p 21

But then

$$\Pr[\overset{A}{Y \text{ is a lin. comb. } Y_1, \dots, Y_{i-1}} \mid \overset{B,\ \ C}{Y_1, \dots, Y_i \in V}]$$

$$\leq \frac{1}{\sigma} \Pr[Y_i \text{ is a lin. comb. } Y_1 \dots Y_{i-1} \mid Y_1 \dots Y_{i-1} \in V]$$

$$P(A|BC) \leq \frac{P(A|B)}{P[C|\bar{B}]}$$

$$\overset{\shortparallel}{P[C]}$$

$$\leq \frac{1}{\sigma} \cdot \left(\frac{1}{1-\mu}\right)^{n-i+1}$$ — adapt proof of Proposition 7

So $$\Pr[Y_1 \dots Y_{\delta n} \text{ not lin. dep.} \mid Y_1 \dots Y_{\delta n} \in V] \leq O\left(\frac{(1-\epsilon_1)^n}{(1-\mu)^{n-\delta n}}\right)$$

$$= o(1).$$

So

$$\Pr\left(Y_1, Y_2, \dots Y_{\delta n} \text{ are lin. indep. vectors in } V \right) \geq \Omega\left(\frac{1}{\sqrt{\mu}}\right)^{\delta n} \sigma^{\delta n}$$

This follows from ⊛ on P22.

Then

$$\Pr[X_1, \dots, X_n \text{ span } V] \leq O(\sqrt{\mu})^{\delta n} \sigma^{-\delta n} \Pr(E_V) \quad ⊛$$

where

$$E_V = \{ X_1, \dots, X_n \text{ span } V \text{ and } Y_1, \dots Y_{\delta n} \text{ are lin. indep. in } V \}$$

Use $\Pr(E_V) = \Pr(X_1 \dots V) \Pr(Y_1 \dots V)$

If E_V occurs then $\exists$ $n-\delta n$ vectors in $X_1, \dots X_n$ which together with $Y_1, \dots Y_{\delta n}$ span V.

Fixing these vectors fixes V. Thus

$$\sum_{V:\, P[X \in V] \sim \sigma} \Pr[E_V] = \sum_{\substack{|S| = n-\delta n \\ X_i : i \in S \\ Y_1, \dots Y_{\delta n}}} \Pr[X_i, i \in S, Y_1, \dots Y_{\delta n}]\, \sigma^{\delta n} \leq \binom{n}{\delta n} \sigma^{\delta n}$$

remaining X_i are in V

So

$$\sum_{V:\, P[X \in V] \sim \sigma} \Pr[X_1, \dots, X_n \text{ span } V] \leq \underbrace{O(\sqrt{\mu})^{\delta n} \binom{n}{\delta n}}$$

use (*) on p 23

Now choose $\delta = \delta(\mu)$ small, and μ small so that $\leq (1-\epsilon)^n$.

$\# \sigma = O(n^2)$ and we are done.

Focus on $\Pr\left(X_v^{(\mu)} = x\right)$

$v = (v_1, \ldots, v_n)$ and $X_v^{(\mu)} = \sum_{j=1}^{n} \eta_j^{(\mu)} v_j$

$$\eta_j^{(\mu)} = \begin{cases} 0 & 1-\mu \\ -1 & \mu/2 \\ 1 & \mu/2 \end{cases}$$

A is an additive set — finite subset of an additive abelian group G.

For our purposes it suffices to take $G = \mathbb{Z}_N$ for a large prime $N \gg \sum_{i=1}^{n} |v_i|$.

Proposition

Let G be a finite group of odd order and $v \in G^n$. Then

(*)

$$\Pr\left(X_v^{(\mu)} = x\right) = \mathbb{E}_{\xi \in G}\left(\cos(2\pi\, \xi * x) \prod_{j=1}^{n} \left(1-\mu+\mu\cos(2\pi\, \xi * v_j)\right)\right)$$

[$\xi * x : G \times G \to \mathbb{R} \backslash \mathbb{Z}$ which is a non-degenerate homomorphism in each component.]

If $G = \mathbb{Z}_p$ then we would take

$\xi * x = \dfrac{\xi x}{p}$, fractional part.

[Previously $\xi \cdot x : G \times G \to S^1$. Use $*$ to differentiate]

RHS(ⓥ 30) =

$$E_{\xi \in G}\left(e^{2\pi \xi * x i} \prod_{j=1}^{n}\left(1-\mu+\mu \cos(2\pi\, \xi * x)\right)\right)$$

$$\left[\, E_{\xi}\left(\sin(2\pi\, \xi * x) \prod_{j=1}^{n}(1-\mu+\mu\cos(2\pi\, \xi * x)\right)\right] = 0.$$

$$\frac{1}{|G|}\sum_{\xi} S(\xi) f(\xi) = \frac{1}{|G|}\sum_{\xi} S(-\xi)\, f(-\xi)$$

$$= -\frac{1}{|G|}\sum_{\xi} S(\xi)\, f(\xi).$$

]

$$1-\mu+\mu\cos(2\pi\xi * v_j) = E_\mu\left(e^{2\pi\xi*(\eta_j^{(\mu)}v_j)i}\right)$$

$$\left[\text{RHS} = 1-\mu+\frac{\mu}{2}\left[\cos(2\pi\xi*v_j)+i\sin(2\pi\xi*v_j)\right]\right.$$
$$\left.+\frac{\mu}{2}\left[\cos(2\pi\xi*v_j) - i\sin(2\pi\xi*v_j)\right]\right]$$

$$\text{RHS}(*30) = E_\xi\left(\exp\left\{-2\pi\xi*x\,i+2\pi i\,\xi*\sum_j\eta_j^{(\mu)}v_j\right\}\right)$$
$$= E_\xi E_\mu\, e^{2\pi i\,\xi*(X_w^{(\mu)}-x)}$$
$$= E_\mu\left(\frac{1}{|G|}\sum_{\xi\in G} e^{2\pi i\,\xi*(X_w^{(\mu)}-x)}\right)$$
$$= E_\mu\left(\mathbb{1}_{X_w^{(\mu)}=x}\right)$$
$$= \Pr\left(X_w^{(\mu)}=x\right).$$

Proposition

(i) $0 \leq \mu \leq \frac{1}{2} \Rightarrow E_\mu = 1 - \mu + \mu \cos(2\pi \xi * \vartheta_0) \geq 0$

(ii) Suppose $0 \leq \mu \leq \frac{1}{4}$

Let $\xi * \vartheta_0 = a + f$, $a \in \mathbb{Z}$, $|f| \leq \frac{1}{2}$

$$E_\mu = 1 - \mu + \mu\left(1 - \frac{(2\pi f)^2}{2!} + \frac{(2\pi f)^4}{4!} - \cdots\right)$$

$$= 1 - \mu\left(\frac{(2\pi f)^2}{2!} - \frac{(2\pi f)^4}{4!} + \cdots\right)$$

$$E_\mu \leq 1 - \mu\left(\frac{(2\pi f)^2}{2!} - \frac{(2\pi f)^4}{4!}\right) \leq 1 - \mu \frac{2\pi^2}{5} f^2 \leq e^{-\frac{2\pi^2 \mu}{5} f^2}$$

$$E_\mu \geq e^{-20\mu f^2}$$

[Mathematics]

Proposition: G is finite of odd order

Let $v \in G^n$.

(I) Domination.

$0 \leq \mu \leq \mu' \leq 1$ and (a) $\mu' \leq \frac{1}{2}$ or (b) $\mu \leq \mu'/4$

$$\Pr[X^{(\mu')}_{vw} = 0] \leq \Pr[X^{(\mu)}_{v} = 0]$$

$vw = v_1 \cdots v_m w_1 \cdots w_m$

(II) Duplication

If $0 \leq \mu \leq 1/2$ then

$$\Pr(X^{(\mu)}_{vw} = 0) \leq \Pr[X^{(\mu/k)}_{v^k} = 0] \quad v^k = vvv \cdots v$$

$\forall\, k \geq 1$

(III) Holder

If $0 \leq \mu \leq \frac{1}{2}$ then

$$\Pr\left[X^{(\mu)}_{v w_1 \dots w_k} = x \right] \leq \prod_{i=1}^{k} \Pr\left(X^{(\mu)}_{v w_i^k} = 0 \right)^{1/k}$$

Proof

Holder

$$\text{LHS} \leq E_\xi \left(\prod_{j=1}^{n} \left(1-\mu+\mu \cos(2\pi \xi * v_j)\right) \times \right.$$

$$\left. \prod_{i=1}^{k} \prod_{\ell} \left(1-\mu+\mu \cos(2\pi \xi * w_{i,\ell})\right) \right)$$

$\leq$ RHS.

We use Holder's inequality which implies $E(Z_1 Z_2 \dots Z_k) \leq \prod_{i=1}^{k} E(Z_i^k)^{1/k}$.

Here $Z_i := \prod_{j=1}^{n} \left(1-\mu+\mu \cos(2\pi \xi * v_j)\right)^{1/k} \prod_{\ell} \left(1-\mu+\mu \cos(2\pi\xi * w_{i,\ell})\right)$.

Domination

$\mu' \leq \frac{1}{2}$ follows from non-negativity

and monotonicity $\downarrow$ in μ of $1 - \mu + \mu \cos(2\pi i\, \xi * v_j)$

On the other hand, if $\mu \leq \mu'/4$ then we use

$$|\cos(\pi\theta)| \leq \frac{3}{4} + \frac{1}{4}\cos(2\pi\theta)$$

and then

$$|1 - \mu' + \mu' \cos(\pi\theta)| \leq \left(1 - \frac{\mu'}{4}\right) + \frac{\mu'}{4}\cos(2\pi\theta).$$

So

$$\mathbb{E}_{\xi} \prod_{j=1}^{n} \left(1 - \mu' + \mu' \cos(2\pi \xi * v_j)\right)$$

$$\leq \mathbb{E}_{\xi} \prod_{j=1}^{n} \left(1 - \frac{\mu'}{4} + \frac{\mu'}{4} \cos(4\pi \xi * v_j)\right)$$

$\forall \mu \leq \frac{\mu'}{4}$

$$\leq \mathbb{E}_{\zeta = 2\xi} \prod_{j=1}^{n} \left(1 - \mu + \mu \cos(2\pi \zeta * v_j)\right)$$

[Random choice of 2ξ = random choice of ξ - $|G|$ odd]

Duplication

$$(1-\mu+\mu\cos(2\pi\theta)) \leq \left(1-\frac{\mu}{k}+\frac{\mu}{k}\cos(2\pi\theta)\right)^k$$

immediately implies duplication inequality.

$k\log\left(1-\frac{t}{k}\right) \geq \log(1-t)$ — concavity of log.

Proposition

Let $v \in G^n$ where G is torsion free and such that $v_i \neq 0$ for at least k of the v_i.

Then for all $0 < \mu \leq 1$ and $x \in G$ we have

$$\Pr\left[X_v^{(\mu)} = x\right] = O\left(\frac{1}{\sqrt{k\mu}}\right)$$

Proof

If $\mu \geq \frac{1}{2}$ then $\Pr\left[X_v^{(\mu)} = x\right] \leq \Pr\left[X_v^{(1/8)} = 0\right]$.

Domination

If $\mu \leq \frac{1}{2}$ then

$$\Pr\left(X_v^{(\mu)} = x\right) \leq \Pr\left(X_{vv}^{(\mu/2)} = 0\right) \quad \text{Duplication}$$

$$\leq \prod_{i=1}^{k} \Pr\left(X_{vv_i^k}^{(\mu/2)} = 0\right)^{1/k} \quad \text{Holder}$$

$$\leq \Pr\left(X_{v_j^k}^{(\mu/2)} = 0\right) \quad \text{for some } j.$$

Now this is simple random walk.

Proof of Proposition 20

Using domination we can assume that $\mu' \leq \frac{1}{4}$ and $x = 0$.

We can also assume that $\mu'/\mu >> 1$ –

[if μ is "large" we use dominance and absorb in constants in O]

Can assume that $G = \mathbb{Z}_p$ for large prime p.

$$f(\xi) = \prod_{j=1}^{n} (1 - \mu' + \mu' \cos(2\pi\, \xi * v_j)) \leq \exp\left\{ -\frac{2\pi^2 \mu'}{5} \sum_j \|\xi * v_j\|^2 \right\}$$

$$g(\xi) = \prod_{j=1}^{n} (1 - \mu + \mu \cos(2\pi\, \xi * v_j)) \geq \exp\left\{ -20\mu \sum_j \|\xi * v_j\|^2 \right\}$$

Must show

$$E_{\mathbb{Z}_p}(f) = O\left(\sqrt{\frac{\mu}{\mu'}}\, E_{\mathbb{Z}_p}(g)\right) + O\left(E_{\mathbb{Z}_p}(g)^{\Omega(\mu'/\mu)}\right).$$

Fix $0 < \alpha \leq 1$.

$f(\xi) \geq \alpha$ implies

$$\exp\left\{-\frac{2\pi^2\mu'}{5}\sum_{j=1}^{n}\|\xi * v_j\|^2\right\} \geq \alpha$$

$$\Rightarrow \left(\sum_{j=1}^{n}\|\xi * v_j\|^2\right)^{1/2} \leq \sqrt{\frac{5}{2\pi^2}}\,\frac{\sqrt{\log 1/\alpha}}{\sqrt{\mu'}}$$

Thus if $\xi_1, \xi_2, \ldots, \xi_m \in S_\alpha := \{\xi \in \mathbb{Z}_p : f(\xi) \geq \alpha\}$

then

$$\left(\sum_{j=1}^{m} \|(\xi_1 + \cdots + \xi_m) * \vartheta_j\|^2 \right) \leq \sqrt{\frac{5}{2\pi^2}}\, m \sqrt{\frac{\log 1/\alpha}{\mu^2}}$$

Triangle inequality:

$$\left(\sum_{j=1}^{n} \|(\xi_1 + \xi_2) * \vartheta_j\|^2 \right)^{1/2} \leq$$

$$\left(\sum_{j=1}^{n} \left(\|\xi_1 * \vartheta_j\| + \|\xi_2 * \vartheta_j\| \right)^2 \right)^{1/2} \leq$$

$$\left(\sum_{j=1}^{n} \|\xi_1 * \vartheta_j\|^2 \right)^{1/2} + \left(\sum_{j=1}^{n} \|\xi_2 * \vartheta_j\|^2 \right)^{1/2}.$$

Now let $m = \lfloor c\sqrt{\mu'/\mu} \rfloor$ for small $c > 0$:

$$g(\xi_1 + \dots + \xi_m) \geq \exp\Big\{-20\mu \sum_{j=1}^{n} \|(\xi_1 + \dots + \xi_m) * \vartheta_j\|^2\Big\}$$

$$\geq \exp\Big\{-20\mu \cdot \frac{5}{2\pi^2} \cdot \lfloor c\sqrt{\mu'/\mu} \rfloor^2 (\log 1/\alpha)/\mu'\Big\}$$

$$> \alpha$$

if $c < \frac{2\pi^2}{100}$.

Thus

$$m\{\xi \in \mathbb{Z}_p : f(\xi) > \alpha\} \leq \{\xi \in \mathbb{Z}_p : g(\xi) > \alpha\}$$

Applying Cauchy-Davenport $|A+B| \geq \min\{|A|+|B|-1, p\}$

we get:

$$\left|\{\xi \in \mathbb{Z}_p : g(\xi) > \alpha\}\right| \geq \min\{m\left|\{\xi \in \mathbb{Z}_p : f(\xi) > \alpha\}\right| - (m-1), p\}$$

$$\Pr(g(\xi) > \alpha) \geq \min\{m \Pr_{\mathbb{Z}_p}(f(\xi) > \alpha) - \frac{m-1}{p}, 1\}$$

If $\alpha > E_{\mathbb{Z}_p}(g)$ then $\Pr_{\mathbb{Z}_p}(g(\xi) > \alpha) < 1$

So

$$\Pr(f(\xi) > \alpha) \leq \frac{1}{m} \Pr(g(\xi) > \alpha) + \frac{1}{p}$$

Integrating over such α

$$\mathbb{E}_{\mathbb{Z}_p}\left(f \mathbb{1}_{\{\alpha \geq \mathbb{E}(g)\}} \right) \leq \frac{1}{m} \mathbb{E}(g) + \frac{1}{p}$$

$$= O\left(\sqrt{\frac{\mu}{\mu'}}\, \mathbb{E}(g) \right).$$

On the other hand

$$f(\xi) \leq g(\xi)^{(100/2\pi^2)\mu'/\mu}$$

and so

$$\mathbb{E}\left(f \mathbb{1}_{\{\alpha < \mathbb{E}(g)\}} \right) \leq \mathbb{E}(g)^{\frac{100}{2\pi^2} \cdot \frac{\mu'}{\mu}}$$

$\square$

Proof of Proposition 14

A tuple $(\omega_1, \omega_2, \dots, \omega_r)$ is <u>k-dissociated</u> if the GAP $[-k,k]^r \cdot (\omega_1, \omega_2, \dots, \omega_r)$ is proper.

Algorithm

Step 0 $r = 0$; $(w_1, w_2, \dots, w_r)$ is trivially $\frac{1}{2}k$-dissociated.

Proposition 29 implies

$$\Pr(X_v^{(1)} = x) \leq \Pr\left(X^{(1/4d)}_{v^{d-r} w_1^{k^2} \cdots w_r^{k^2}} = 0\right) \quad (*)$$

$\Big(r = 0;$ duplication $\leq P[X^{1/d}_{v^d} = 0] \leq$ dominance $\Big)$

Step 1

$\nu = \# i : (w_1, w_2, \dots, w_r, v_i)$ is $\frac{k}{2}$-dissociated.

If $\nu \leq k^2$, halt.

[On termination for all but $\leq k^2$ of $v_1, \dots, v_n$, $\exists\, a = a(v_i) \in [1, k]$ such that $a v_i \in [-k, k]^r \cdot (w_1, \dots, w_r)$.]

Step 2

Write $v^{d-r} w_1^{k^2} \cdots w_r^{k^2} = v^{d-r-1} a\, w_1^{k^2} \cdots w_r^{k^2} b_1 b_2 \cdots b_{k^2}$

where $b_1, \dots, b_{k^2}$ are k-dissociated from $w_1, \dots, w_r$.

Then

$$\Pr_x\left[X^{(1/4d)}_{v^{d-r} w_1^{k^2} \cdots w_r^{k^2}} = 0 \right] \le \prod_{i=1}^{k^2} \underbrace{\Pr_i\left[X^{(1/4d)}_{v^{d-r-1} w_1^{k^2} \cdots w_r^{k^2} b_i^{k^2}} \right]^{1/k^2}}_{\text{Choose } b_i \text{ to maximise}}$$

Return to step 1 with $r \leftarrow r+1$; $w_{r+1} \leftarrow b_i$

We only need to prove that we can choose δ_d such that if $\Pr[X_v^{(1)} = x] > \delta_d k^{-d}$ then we halt before r reaches d.

Suppose that we reach step 1 and we have k-dissocossiated tiple $(w_1, w_2, \dots, w_d)$ such that:

$$P[X_v^{(1)} = x] \leq P[X^{(1)(4d)}_{w_1^{b^2} \cdots w_d^{b^2}} = 0]$$

Let

$$\Gamma = \{(m_1, m_2, \dots, m_d) : m_1 \omega_1 + \dots + m_d \omega_d = 0\}.$$

Then, by independence,

$$P[X_v^{(1)} = x] \leq \sum_{(m_1, \dots, m_d) \in \Gamma} \prod_{j=1}^{d} P\left(X_{1/k^2}^{(1/4d)} = m_j\right)$$

Note that

(1) $P[X_{1/k^2}^{(1/4d)} = m] = P[X_{1/k^2}^{(1/4d)} = -m]$ and $\searrow$ with m

$$= \Theta_d(1/k)$$

Thus

$$\Pr[X^{(1/4d)}_{1k^2} = m] = O_d\Big(\frac{1}{k}\sum_{m' \in m + (-k/2,\, k/2)} P(X^{(1/4d)}_{1k^2} = m')\Big)$$

and then

$$\Pr[X^{(1)}_v = x] \le O_d\Big(k^{-d}\sum_{m_1,\dots,m_d \in \Gamma}\ \sum_{\substack{(m'_1,\dots,m'_d)\in \\ (m_1,\dots,m_d)+(-\frac{k}{2},\frac{k}{2})^d}}\ \prod_{v=1}^{d} P[X^{(1/4d)}_{1k^2} = m'_v]\Big)$$

Now $(w_1,\dots,w_d)$ $k/2$-dissociated $\Rightarrow$ distinct.

But then

$$\Pr[X^{(1)}_v = x] \le O_d(k^{-d})$$ and we

take δ_d larger than hidden constant in .