Plus petite valeur singulière d'une matrice aléatoire. Premiers résultats

I/ Généralités

Dans toute la suite on se donne des entiers n, N tq

$$\boxed{N \geq n \geq 1}$$

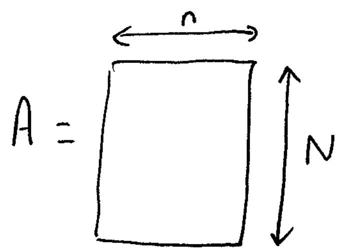
Les matrices considérées seront des matrices $N \times n$ (lignes × colonnes)

On travaillera avec les structures euclidiennes usuelles $(\mathbb{R}^n, |\cdot|)$ et $(\mathbb{R}^N, |\cdot|)$

Ainsi A est une matrice $N \times n$

$$\Updownarrow$$

$$A : \ell_2^n \longrightarrow \ell_2^N$$



On peut voir A comme un plongement de ℓ_2^n dans un plus grand espace ℓ_2^N.

Rq: Différence avec des études précédentes : ici on veut aussi étudier le cas des matrices carrés $n \times n$ $(N = n)$

Def : Soit A une matrice $N \times n$. Les valeurs singulières de A sont les valeurs propres de $\sqrt{{}^tAA} \in \mathcal{M}_n(\mathbb{R})$, que l'on range en ordre décroissant

$$s_1(A) \geq s_2(A) \geq \dots \geq s_n(A) \geq 0$$

Classique : $$s_1(A) = \max_{|x|=1} |Ax| = \|A\|_{\ell_2^n \to \ell_2^N}$$

$\longrightarrow$ Nous allons nous intéresser à $s_n(A)$

On dit que A est "inversible" si $s_n(A) > 0$

On s'intéresse donc à l'inversibilité de A.

Fait immédiat : $\boxed{s_n(A) = \min_{|x|=1} |Ax|}$

Dans la suite on notera
$$S^{n-1} = \{x \in \mathbb{R}^n ; |x| = 1\}$$
$$S^{N-1} = \{x \in \mathbb{R}^N , |x| = 1\}$$

On a :

$s_n(A) \neq 0 \Leftrightarrow A$ est injective

et alors on a :
$$s_n(A) = \frac{1}{\|A^{-1}_{|Im(A)}\|_{Im(A) \to \ell_2^n}}$$
$$Im(A) \subset \ell_2^N$$

Position du problème

A est une matrice $N \times n$ dont les entrées sont des variables aléatoires indépendantes (entrées) + conditions techniques.

Conjecture de Von Neumann : lorsque $N = n \longrightarrow +\infty$ on a
$$s_n(A) \sim \frac{1}{\sqrt{n}} \quad \text{en grande proba}$$
variable aléatoire

↓ résultat asymptotique (en g^al on veut mieux) quantitatif

Cas d'une matrice gaussienne (entrées iid gaussiennes standard)

→ On a vu que lorsque : $n \leq c(\varepsilon) N$ ($c(\varepsilon) < 1$ une certaine constante numérique dépendant de ε)

alors
$$\mathbb{P}\left(\forall x \in S^{n-1}, \ (1-\varepsilon) m \leq |Ax| \leq (1+\varepsilon) m \right) \geq 1 - e^{-\tilde{c}(\varepsilon) n}$$
$$m = \int |x| \, d\gamma_N \simeq \sqrt{N}$$

En particulier pour $\varepsilon = \frac{1}{2}$

∃ des constantes numériques $c_1, c_2, c, C > 0$ tq
$\forall n, N \geq 1$ avec $n \leq cN$ et A matrice gaussienne standard $N \times n$
on a :
$$\mathbb{P}\left(c_1 \sqrt{N} \leq s_n(A) \leq s_1(A) \leq c_2 \sqrt{N} \right) \geq 1 - e^{-cN}$$

en particulier : $\mathbb{P}\left(s_n(A) \leq c_1 \sqrt{N} \right) \leq e^{-cN}$

<u>question</u> : → que se passe-t-il lorsque $n = N$ (ou n proche de N) ?
A-t-on $s_n(A) \sim \frac{1}{\sqrt{n}}$?

<u>Résultat connu</u> : si A matrice gaussienne standard <u>$n \times n$</u>
alors
$$(*) \quad \mathbb{P}\left(s_n(A) \leq \frac{\varepsilon}{\sqrt{n}} \right) \leq C\varepsilon, \ \forall \varepsilon$$
$$(**) \quad \mathbb{P}\left(s_n(A) \geq \frac{t}{\sqrt{n}} \right) \leq C e^{-t^2} \quad \forall t \geq 0$$

On a bien $s_n(A) \simeq \frac{1}{\sqrt{n}}$

→ le point important est $(*)$
Inversibilité d'une matrice gaussienne.

Pour le point $(**)$, en gal on sait même estimer
$$\mathbb{P}(\underbrace{s_1(A)}_{= \|A\|} \geq \dots) \leq \dots$$

Dans la suite on va considérer une matrice dont les entrées sont indépendants et
→ centrés et de variance 1
→ ψ_2 avec constante B
ou
moment d'ordre 4 fini

Toutes les estimés vont dépendre de B. L'important est que les constantes ne dépendent pas de N et n.

II/ Rappels sur les variables ψ_2

Une variable aléatoire ξ est ψ_2 si $\xi : \Omega \longrightarrow \mathbb{R}$ est $\psi_2(\mathbb{P})$

Rq : Soit $\mathcal{M}_\xi$ est la loi de ξ sur $\mathbb{R}$, cela revient à dire que la fonction $\begin{array}{l}\mathbb{R} \longrightarrow \mathbb{R} \\ t \longrightarrow t\end{array}$ est $\psi_2(\mathcal{M}_\xi)$

Bref, cela revient à dire que $\exists a > 0$ tq $\mathbb{E}\, e^{a|\xi|^2} < +\infty$

Rappel : alors $\exists \lambda_0 > 0$ tq $\mathbb{E}\, e^{\left(\frac{\xi}{\lambda_0}\right)^2} \leq 2$

Prop : Soit ξ une variable aléatoire <u>centrée</u> ($\mathbb{E}\xi = 0$)
Alors les propriétés suivantes sont équivalentes

1) $\mathbb{E}\, e^{\left(\frac{\xi}{a}\right)^2} \leq 2$
2) $\mathbb{P}(|\xi| > t) \leq C e^{-ct^2}$, $\forall t \geq 0$
3) $\forall p \geq 1$, $\left(\mathbb{E}|\xi|^p\right)^{1/p} \leq K\sqrt{p}$
4) $\mathbb{E}\, e^{\lambda\xi} \leq e^{b\lambda^2}$, $\forall \lambda \in \mathbb{R}$

où les constantes dans chaque de ces propriétés dépendent seulement des constantes dans l'une des autres propriétés.

Rq : On peut se ramener à une variable centrée en prenant $\xi - \mathbb{E}\xi$.
Notez que pour une variable centrée, la propriété 2) revient à de la concentration autour de la moyenne.

Demo : Déjà vu ! Vraiment ?
On a vu 1) $\Leftrightarrow$ 2) $\Leftrightarrow$ 3) avec les correspondances entre constantes.

Dans le cas gal (non centré) on a vu que cela était équivalent à

4') $\mathbb{E}\, e^{\lambda\xi} \leq \tilde{C} e^{b\lambda^2}, \quad \forall \lambda > 0$

⚠ Ici $\tilde{C} = 1$ (Important pour la tensorisation)

Rq : 4) ne peut être vrai que pour des variables centrées

En effet $\mathbb{E}\, e^{\lambda\xi} = 1 + \lambda\, \mathbb{E}\xi + o(\lambda)$

$$e^{b\lambda^2} = 1 + o(\lambda)$$

Démo de 1) ⇒ 4)

• Supposons d'abord que ξ est symétrique (ξ a la même loi que $-\xi$)

Alors $\mathbb{E}\, e^{\lambda\xi} = \mathbb{E}\, e^{-\lambda\xi} = \mathbb{E}\, \mathrm{ch}(\lambda\xi) \leq \mathbb{E}\, e^{\lambda^2\xi^2/2}$

→ Si $\lambda^2 \leq \frac{2}{a^2}$, alors $\mathbb{E}\, e^{\lambda\xi} \leq \mathbb{E}\, e^{\lambda^2\xi^2/2} \leq \left(\mathbb{E}\, e^{\xi^2/a^2}\right)^{\frac{\lambda^2 a^2}{2}}$ Jensen $\frac{2}{\lambda^2 a^2} \geq 1$

$$\leq 2^{\frac{\lambda^2 a^2}{2}} = e^{b_1\lambda^2}$$

avec $b_1 = a^2 \log(2)/2$

→ Si $\lambda^2 \geq \frac{2}{a^2}$, comme $\lambda\xi \leq \frac{\xi^2}{a^2} + a^2\lambda^2/4$ on a

$$\mathbb{E}\, e^{\lambda\xi} \leq 2\, e^{a^2\lambda^2/4} \quad \& \quad 2 \leq e^2 \leq e^{\lambda^2 a^2}$$

$$\leq e^{b_2\lambda^2}$$

avec $b_2 = \frac{5}{4} a^2$

Donc pour $b = \max(b_1, b_2)$ on a : $\mathbb{E}\, e^{\lambda\xi} \leq e^{b\lambda^2}, \ \forall \lambda \in \mathbb{R}$

• Si ξ n'est pas symétrique ?

Soit ξ' une copie indépendante de ξ. Comme $\mathbb{E}\xi = \mathbb{E}\xi' = 0$

on a : $\mathbb{E}\, e^{\lambda\xi} = \mathbb{E}\, e^{\lambda\xi} e^{\lambda\mathbb{E}\xi'} \overset{\text{Jensen}}{\leq} \mathbb{E}\, e^{\lambda(\xi - \xi')}$

et $\xi - \xi'$ est ψ_2 avec constante $\sqrt{2}a$ puisque $|\xi - \xi'|^2 \leq 2(|\xi|^2 + |\xi'|^2)$

et donc $\mathbb{E}\, e^{(\xi-\xi')^2/4a^2} \leq \mathbb{E}\, e^{\xi^2/2a^2}\, \mathbb{E}\, e^{\xi'^2/2a^2} \leq \sqrt{2} \times \sqrt{2} = 2$

Conséquence immédiate

Prop : Soit $\xi_1, \dots, \xi_n$ des variables centrées indépendantes et ψ_2 pour une même constante $b>0$: $\mathbb{E}\, e^{\lambda \xi_i} \leq e^{b^2\lambda^2}$, $\forall \lambda \in \mathbb{R}$.
Alors, si $a \in S^{n-1}$, la variable $a_1\xi_1 + \dots + a_n \xi_n$ est aussi ψ_2 avec la même constante, et donc

$$\forall t \geq 0, \quad \mathbb{P}\left(\left| \sum_{j=1}^{n} a_j \xi_j \right| \geq t \right) \leq 2 e^{-ct^2}$$

avec c dépendant de b.

Démo : Pour $\lambda \in \mathbb{R}$ et $a \in \mathbb{R}^n$ on a, par indépendance,

$$\mathbb{E}\, e^{\lambda \sum a_j \xi_j} = \prod_{j=1}^{n} \mathbb{E}\, e^{\lambda a_j \xi_j}$$
$$\leq \prod_{j=1}^{n} e^{b^2 a_j^2 \lambda^2} = e^{b^2 (\sum_{j=1}^n a_j^2) \lambda^2} \quad \blacksquare$$

Dans la suite, on va considérer des matrices $N \times n$ avec des entrées ξ_{ij} qui sont centrées et, parfois, ψ_2.
Les estimés peuvent dépendre des constantes caractérisant le côté ψ_2 (les constantes de 1), 2), 3) ou 4)), mais pas de N et n

On se fixe donc une borne sur les constantes ψ_2. Pour cela on choisit l'une des caractérisations. Par commodité on peut prendre 3)).

Dans toute la suite, $B>0$ est une constante fixée.

<u>Def</u> (Hypothèse $H_1(B)$)

On dit que la variable aléatoire ξ vérifie $H_1(B)$ si ξ est centrée, de variance 1 et ψ_2 pour la constante B, càd

$$H_1(B) \begin{cases} \mathbb{E}\,\xi = 0 \\ \mathbb{E}\,\xi^2 = 1 \\ \forall p \geq 1, \quad (\mathbb{E}|\xi|^p)^{1/p} \leq B\sqrt{p} \end{cases}$$

On aura parfois besoin d'avoir une estimation de $\|A\|_{\ell_2^n \to \ell_2^N}$.

Le résultat suivant repose sur une méthode déjà vue :

<u>Prop A</u> : Soit A une matrice ~~aléatoire~~ aléatoire $N \times n$ à entrées indépendantes ξ_{ij} vérifiant $H_1(B)$. Alors

$$\forall t \geq C_0, \quad \mathbb{P}\left(\|A\|_{\ell_2^n \to \ell_2^N} > t\sqrt{N} \right) \leq e^{-c_0 t^2 N}$$

où $c_0, C_0 > 0$ sont des constantes dépendant seulement de B

<u>Démo</u> : Soit $\mathcal{N}$ un $\frac{1}{2}$-réseau de S^{N-1} avec $|\mathcal{N}| \leq 5^N$

et $\mathcal{M}$ " " " S^{n-1} " $|\mathcal{M}| \leq 5^n \leq 5^N$

On a alors (<u>Exercice</u>)

$$\|A\|_{\ell_2^n \to \ell_2^N} = \max_{\substack{x \in S^{n-1} \\ y \in S^{N-1}}} |Ax \cdot y|$$

$$\leq 4 \max_{\substack{x \in \mathcal{M} \\ y \in \mathcal{N}}} |Ax \cdot y|$$

Pour $x \in S^{n-1}$ on a : $\forall i \leq N$

$$(Ax)_i = \sum_{j=1}^{n} x_j \xi_{ij}$$

D'après la prop, on a : $(Ax)_i =: X_i \in H_1(B)$

Ensuite : pour $y \in S^{N-1}$, $Ax \cdot y = \sum_{i=1}^{N} y_i X_i \in H_1(B)$

encore d'après la prop.

Donc $\forall t \geq 0$, $\mathbb{P}(|Ax \cdot y| \geq t) \leq 2e^{-ct^2}$ avec $c = c(B)$

soit encore

$$\forall t \geq 0, \quad \mathbb{P}(|Ax \cdot y| \geq t\sqrt{N}) \leq 2e^{-ct^2 N} \quad (*)$$

et ceci $\forall x \in S^{n-1}$ et $y \in S^{N-1}$. En utilisant $\mathbb{P}(\cup \ldots) \leq \sum \mathbb{P}(\ldots)$ on en déduit que

$$\mathbb{P}(\|A\|_{\ell_2^n \to \ell_2^N} > t\sqrt{N}) \leq |\mathcal{N}||\mathcal{M}| \times 2e^{-c\left(\frac{t}{4}\right)^2 N}$$

$$\leq 2\, 5^{2N} e^{-\tilde{c}t^2 N}$$

$$\leq e^{-\frac{\tilde{c}}{2}t^2 N} \quad \text{si } t > 6(\tilde{c}).$$

Rq : On peut aussi directement remarquer que $Ax \cdot y = \sum_{i=1}^{N}\sum_{j=1}^{n} x_j y_i \xi_{ij}$ et $\sum x_i^2 y_j^2 = 1$, puis utiliser la prop pour arriver à $(*)$. $\blacksquare$

III/ Hypothèse générale et cas des matrices strictement rectangulaires

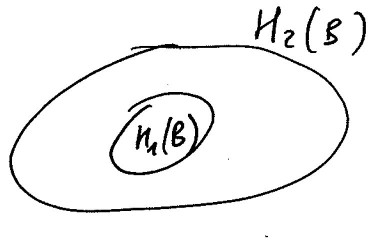
On va travailler avec des matrices qui ont à entrées plus générales que ψ_2. On dit qu'une v.a. ξ vérifie $H_2(B)$ si

$$H_2(B) \begin{cases} \mathbb{E}\xi = 0, \quad \mathbb{E}\xi^2 = 1 \\ \text{et} \quad \mathbb{E}\xi^4 \leq (2B)^4 \end{cases}$$

$\xi \in H_2(B) \Leftrightarrow$ ξ v.a. centrée de variance 1 et ayant un moment d'ordre 4 (borné par une cte dépendant de B)

$$\xi \in H_1(B) \Rightarrow \left(\mathbb{E}\,\xi^4\right)^{1/4} \leq \sqrt{4}\, B$$

Donc $\xi \in H_1(B) \Rightarrow \xi \in H_2(B)$



En fait le cas le plus important est le cas de variables ψ_2, càd le cas où $\xi \in H_1(B)$

Cependant, il est interessant de voir qu'on a souvent besoin de moins

Cas typique de variables vérifiant $H_1(B)$ [ψ_2]

→ ξ gaussiennes standard

→ ξ = Bernoulli ± 1

$$\mathbb{P}(\xi = 1) = \mathbb{P}(\xi = -1) = \frac{1}{2}$$

Plus généralement, ξ variable bornée (la cte B dépendant alors de la borne) → centrée et de variance 1.

On va montrer le résultat suivant

theo A

Soit $K \geq 1$. Il existe des constantes $c_1, c_2, c_2' > 0$ (dépendant de K et B) et $\delta_0 \in]0,1[$ tel que, pour toute matrice aléatoire A $N \times n$ à entrées indep. $H_2(B)$ avec $\boxed{n \leq \delta_0 N}$, on a :

$$\mathbb{P}\left(s_n(A) \leq c_1 \sqrt{N} \text{ et } \|A\|_{\ell_2^n \to \ell_2^N} \leq K\sqrt{N} \right) \leq e^{-c_2 N}$$

Si de plus les entrées sont $H_1(B)$ on a

$$\mathbb{P}\left(s_n(A) \leq c_1 \sqrt{N} \right) \leq e^{-c_2' N}$$

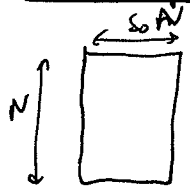
Rem : la propriété " $\mathbb{P}(s_n(A) \le c\sqrt{N}) \le e^{-cN}$ "
est très forte puisqu'on a :

" $s_n(A) \ge c\sqrt{N}$ " en grande proba "

On verra en gal que " $s_n(A) \ge \frac{c}{\sqrt{n}}$ en grande proba "

Mais ici on a des matrices <u>rectangulaires</u> strictes

$\underset{\text{constante fixée}}{n \le \delta_0 N}$



→ Notez qu'on retrouve un résultat ~~vu~~ pour les matrices gaussiennes standards (on avait même $s_n(A) \simeq \sqrt{N}$)

Pour démontrer ce résultat, on va utiliser un résultat dit de " petite boule "

<u>Lemme A</u>

Soit $\xi_1, \dots, \xi_n$ des variables indep $H_2(B)$. Alors il existe $\mu \in]0,1[$ dépendant seulement de B tq $\forall a = (a_1, \dots, a_n) \in S^{n-1}$ tq

$$\mathbb{P}\left(\left| \sum_{i=1}^{n} a_i \xi_i \right| < \frac{1}{2} \right) \le \mu$$

<u>Démo</u>

On commence par symétriser.

Soit $\varepsilon_1, \dots, \varepsilon_n$ des variables de Bernoulli ± 1 <u>indep</u>, et indépendants de $(\xi_1, \dots, \xi_n)$

Alors :

Fait (principe de symétrisation)

$$\mathbb{E}\left|\sum_{i=1}^n a_i\xi_i\right|^4 \le 16\,\mathbb{E}\left|\sum_{i=1}^n \varepsilon_i a_i \xi_i\right|^4$$

Démo Soit $\xi'_1,\dots,\xi'_n$ des variables indep avec $\xi'_i \sim \xi_i$ et indépendantes de $(\xi_1,\dots,\xi_N,\varepsilon_1,\dots,\varepsilon_N)$

on a, comme $\mathbb{E}\xi_i = \mathbb{E}\xi'_i = 0$, par Jensen,

$$\left(\sum_i a_i\xi_i\right)^4 \le \mathbb{E}_{\xi'}\left[\sum_i a_i(\xi_i-\xi'_i)\right]^4$$

Donc :

$$\mathbb{E}\left(\sum a_i\xi_i\right)^4 \le \mathbb{E}\left(\sum a_i(\xi_i-\xi'_i)\right)^4$$

La variable $X_i := \xi_i - \xi'_i$ est symétrique ($X_i \sim -X_i$) et donc (exo) $\varepsilon_i X_i \sim X_i$. Par indépendance on a :

$$\sum_i a_i X_i \sim \sum_i \varepsilon_i a_i X_i$$

Donc

$$\mathbb{E}\left(\sum_i a_i\xi_i\right)^4 \le \mathbb{E}\left(\sum_i \varepsilon_i a_i\xi_i - \sum_i \varepsilon_i a_i \xi'_i\right)^4$$

En utilisant que $(a+b)^4 \le 8(a^4+b^4)$ et $\sum \varepsilon_i a_i\xi_i \sim \sum(-\varepsilon_i)a_i\xi'_i$ on obtient le résultat ∎

Reprenons la démo du Lemme A. Posons $S = \sum_{i=1}^N a_i\xi_i$

On a :

$$\begin{aligned}
\mathbb{E}S^4 &\overset{\text{Fait}}{\le} 16\,\mathbb{E}\left(\sum_{i=1}^n \varepsilon_i a_i\xi_i\right)^4 \\
&= 16\,\mathbb{E}_{(\xi_1\dots\xi_N)}\mathbb{E}_{(\varepsilon_1\dots\varepsilon_N)}\left(\sum_{i=1}^n \varepsilon_i a_i\xi_i\right)^4 \\
&\le 16B^4\,\mathbb{E}\left[\sum_{i=1}^n a_i^2\xi_i^2\right]^2 \\
&= 16\cdot 3\,\mathbb{E}\sum_{i,k=1}^n a_i^2 a_k^2 \xi_i^2\xi_k^2 \\
&\le 16\times 3\sum_{i,k}^n a_i^2 a_k^2 \,(2B)^4 \\
&= C\left(\sum_{i=1}^n a_i^2\right)^2
\end{aligned}$$

Khintchine pour les Bernoulli $L^4 \leftrightarrow L^2$

Hölder

avec C dépendant de B.

On utilise alors

c'est Hölder !

Fait (Inégalité de Paley-Zygmund)

Si Z est une variable aléatoire positive, alors $\forall \theta \in [0,1]$

$$\mathbb{P}(Z \geqslant \theta\, \mathbb{E} Z) \geqslant (1-\theta)^2 \frac{(\mathbb{E} Z)^2}{\mathbb{E}(Z^2)}$$

Démo

$$\begin{aligned}\mathbb{E} Z &= \mathbb{E}(Z \mathbb{1}_{Z<\theta \mathbb{E} Z}) + \mathbb{E}(Z \mathbb{1}_{Z \geqslant \theta \mathbb{E} Z}) \\ &\leqslant \theta\, \mathbb{E} Z + \mathbb{E}(Z \mathbb{1}_{Z\geqslant \theta \mathbb{E} Z}) \\ &\leqslant \theta\, \mathbb{E} Z + \sqrt{\mathbb{E} Z^2\, \mathbb{P}(Z \geqslant \theta \mathbb{E} Z)}\end{aligned}$$

Hölder ■

On a alors

$$\mathbb{P}(|S| \geqslant \tfrac{1}{2}) = \mathbb{P}(S^2 \geqslant \tfrac{1}{4})$$

$$\mathbb{E} S^2 = \sum_{k=1}^{n} a_k^2 = 1$$

par hypothèse.

Paley-Zygmund avec $Z = S^2$, $\lambda = \frac{1}{4}$

$$\geqslant \left(\tfrac{3}{4}\right)^2 \frac{1}{\mathbb{E} S^4}$$

$$\geqslant \tilde{c}(B) \quad \text{constante dépendant de } B$$

$\tilde{c}(B) \in \left]0,1\right]$

On prend $\mu = 1 - \tilde{c}(B) \in \left]0,1\right[$. ■

L'étape suivante importante est une estimation individuelle, pour chaque vecteur.

Prop B : Il existe $\eta, \nu \in \left]0,1\right[$ dépendant de B tel que, pour toute matrice A $N \times n$ à entrée indep $H_2(B)$ on a, $\forall x \in S^{n-1}$

$$\mathbb{P}(|Ax| < \eta \sqrt{N}) \leqslant \nu^N$$

Rq : Notez que ce résultat s'applique à tout $N \geqslant n$ (en particulier au cas $N = n$)

<u>Démo</u> : Soit $\mu \in]0,1[$ constante ~~(~~dépendant seulement de B) du <u>lemme A</u>.

Pour $i \leq N$, ~~max~~ et $x \in S^{n-1}$) $\quad (Ax)_i = \sum_{j=1}^{n} a_j \underbrace{\xi_{ij}}$ variables indep $H_2(B)$

Donc d'après le <u>lemme A</u> on a :

$$\forall i \leq N, \quad \forall x \in S^{n-1}$$
$$\mathbb{P}\left(|(Ax)_i| < \tfrac{1}{2} \right) \leq \mu$$

On travaille maintenant avec $x \in S^{n-1}$ fixe :

Soit $\eta \in]0, \frac{1}{3}]$ que l'on fixera plus loin

Supposons que $|Ax| < \eta\sqrt{N}$ et soit $J = \{ i \leq N ;\ |(Ax)_i| < \frac{1}{2} \}$

alors $\eta^2 N \geq |Ax|^2 \geq \sum_{i \notin J} ((Ax)_i)^2 \geq \frac{1}{4} |J^c|$

Donc $|J| \geq (1-4\eta^2)N$

Soit $\mathcal{P}_\eta = \{ I \subset \{1, \dots, N\} ;\ |I| \geq (1-4\eta^2)N \}$

On a :

$$\mathbb{P}(|Ax| < \eta\sqrt{N}) \leq \mathbb{P}\left(\exists I \in \mathcal{P}_\eta ;\ \forall i \in I,\ |(Ax)_i| < \tfrac{1}{2}\right)$$

$$\leq \sum_{I \in \mathcal{P}_\eta} \mathbb{P}\left(\forall i \in I,\ |(Ax)_i| < \tfrac{1}{2}\right)$$

V.a. <u>indépendantes</u> pour $\neq i$

$$\leq |\mathcal{P}_\eta| \, \mu^{\frac{N}{2}}$$

($\frac{N}{2} \overset{\text{car}}{<} (1-4\eta^2)N$)

$\Downarrow$

$\mu^{(1-4\eta^2)N} \leq \mu^{N/2}$

Par Stirling (immédiat)

$$\exists c > 0 \text{ tq } \forall n \geq k \geq 1$$
$$\binom{n}{k} \leq \left(\frac{cn}{k}\right)^k$$

Donc

$$|\mathcal{P}_\eta| \leq |\{ I \subset \{1,\dots,N\} \ ; \ |I| \geq (1-4\eta^2)N \}|$$
$$= |\{ I \subset \{1,\dots,N\} \ ; \ |I| \leq 4\eta^2 N \}|$$
$$\leq 4\eta^2 N \binom{N}{4\eta^2 N}$$
$$\leq 4\eta^2 N \left(\frac{c}{4\eta^2}\right)^{4\eta^2 N}$$

c cte numérique

$4\eta^2 N \leq e^{4\eta^2 N}$

$$\leq e^{4\eta^2 (\log(\frac{c}{4\eta^2}) + 1) N}$$

$\eta \longrightarrow 4\eta^2 \left(\log\left(\frac{c}{4\eta^2}\right) + 1\right)$ tend vers 0 losque $\eta \to 0$

On fixe un η tq cette fonction est $\leq \frac{1}{4} \log \frac{1}{\mu}$

Alors $|\mathcal{P}_\eta| \leq \left(\frac{1}{\mu}\right)^{N/4}$

On en tire que

$$\mathbb{P}(|Ax| < \eta\sqrt{N}) \leq \mu^{N/4} = (\mu^{1/4})^N$$

on pose $\nu = \mu^{1/4} \in]0,1[$ ■

On est maintenant en mesure de démontrer le théorème A

Démo du théo. A

Soit $\eta, \nu \in]0,1[$ provenant de la Prop B (dépendant de B)

Rappel : $K \geq 1$ est une constante qcq fixée.

On se donne $\varepsilon > 0$ que l'on fixera plus loin.

Soit $\mathcal{N}$ un ε-réseau de S^{n-1} avec $|\mathcal{N}| \leq (1 + \frac{2}{\varepsilon})^n$

Supposons qu'on est dans l'événement

$s_n(A) = \min_{x \in S^{n-1}} |Ax| \leq \frac{\eta}{2}\sqrt{N}$ et $\|G\|_{\ell_2^n \to \ell_2^N} \leq K\sqrt{N}$

alors $\exists x_0 \in S^{n-1}$ tq $|Ax_0| \leq \frac{\eta}{2}\sqrt{N}$

als $\exists y \in \mathcal{N}$ tq $|x-y| \leq \varepsilon$ et donc

$$|Ay| \leq |Ax| + \varepsilon \|A\|$$
$$\leq \frac{\eta}{2}\sqrt{N} + \varepsilon K \sqrt{N}$$

on fixe $\varepsilon_0 := \frac{\eta}{4K}$

on a als $\exists y \in \mathcal{N}$ tq $|Ay| < \eta\sqrt{N}$

Donc

$$\mathbb{P}\Big(s_n(A) \leq \underbrace{\tfrac{\eta}{2}}_{c_1}\sqrt{N} \text{ et } \|A\|_{\ell_2^n \to \ell_2^N} \leq K\sqrt{N} \Big)$$

$$\leq \mathbb{P}(\exists y \in \mathcal{N},\ |Ay| < \eta\sqrt{N})$$

$$\leq |\mathcal{N}|\, \nu^N \qquad \text{d Prop B}$$

$$= e^{cn} \cdot e^{-\tilde{c}N} \qquad \text{avec } c = \log\left(1 + \frac{8K}{\eta}\right) > 0$$

dépend de B et K.

$\tilde{c} = -\log(\nu)$ dépend de B > 0

$$\leq e^{-\frac{\tilde{c}}{2}N}$$

si $n \leq \underbrace{\frac{\tilde{c}}{2c}}_{\delta_0 \text{ dépendant de } B \text{ et } K.} N$

Dans le cas où on suppose $H_1(B)$, on utilise la Prop A.
En choisissant $K = C_0$ (qui dépend seulement de B) on a :

$$\mathbb{P}(\|A\| > K\sqrt{N}) \leq e^{-C_0 N}$$

Donc
$$\mathbb{P}(s_n(A) \leq c_1\sqrt{N}) \leq \mathbb{P}(s_n(A) \leq c_1\sqrt{N} \text{ et } \|A\| \leq K\sqrt{N}) + \mathbb{P}(\|A\| > K\sqrt{N})$$

$$\leq e^{-c_2 N} + e^{-C_0 N}$$

$$\leq e^{-c_2' N}$$

en choisissant $c_2' > 0$ assez petit (en fonction de c_2 et C_0)

$\blacksquare$