

SORBONNE UNIVERSITÉ

TRAVAUX D'ÉTUDE ET DE RECHERCHE

---

## **Autour du théorème de Dvoretzky**

---

Mathieu GALLO

*Enseignant* : Omer Friedland

date



## Partie 1

La genèse du théorème de Dvoretzky provient d'une conjecture proposée par Grothendieck en 1956, inspiré par le théorème de Dvoretzky-Rogers (1950). Dvoretzky répondra positivement à la conjecture en 1960, aboutissant au résultat suivant :

**Théorème 1.** *Il existe une fonction  $k : ]0, 1[ \times \mathbb{N} \rightarrow \mathbb{N}$ , tel que  $\forall \varepsilon \in ]0, 1[, k(\varepsilon, n) \xrightarrow{n \rightarrow \infty} \infty$  et pour tout  $n \in \mathbb{N}$  et tous compact convexe symétrique  $K \subset \mathbb{R}^n$ , il existe un sous espace  $V \subset \mathbb{R}^n$  tel que :*

$$(i) \dim V = k(\varepsilon, n)$$

$$(ii) \exists r > 0 \text{ tel que, } r.(V \cap B_2^n) \subset V \cap K \subset (1 + \varepsilon)r.(V \cap B_2^n)$$

V. Milman en 1971 donna une nouvelle preuve du théorème de Dvoretzky en utilisant le phénomène de concentration de la mesure, il a de plus amélioré le théorème en donnant une estimation de la dépendance en  $n$  pour la dimension de  $V$ ,  $k(\varepsilon, n) \geq c(\varepsilon) \cdot \log(n)$ .

**Théorème 2.** *Pour toute  $\varepsilon > 0$ , il existe une constante  $c > 0$  tel que pour tout  $n \in \mathbb{N}$  et pour tous corps convexe symétrique  $K \subset \mathbb{R}^n$ , il existe un sous espace  $V \subset \mathbb{R}^n$  tel que :*

$$(i) \dim V \geq c \cdot \log(n)$$

$$(ii) \exists r > 0 \text{ tel que, } r.(V \cap B_2^n) \subset V \cap K \subset (1 + \varepsilon)r.(V \cap B_2^n)$$

Il existe une reformulation du théorème en terme de norme.

**Théorème 3.** *Pour tout  $\varepsilon > 0$  il existe  $c > 0$  tel que pour toute  $n \in \mathbb{N}$  et pour toute norme  $\|\cdot\|$  sur  $\mathbb{R}^n$  alors  $l_2^k$  est  $(1 + \varepsilon)$ -isomorphe à  $(\mathbb{R}^n, \|\cdot\|)$  pour un  $k \geq c \cdot \log(n)$ .*

Nous allons montrer que ses deux derniers théorèmes sont équivalents.

(2)  $\Rightarrow$  (3) Posons  $K = \text{Adh}(B_{\|\cdot\|}(0, 1)) = \{x \in \mathbb{R}^n \mid \|x\| \leq 1\}$  et appliquons le théorème 2, celui-ci nous procure un sous-espace  $V$  de  $\mathbb{R}^n$ , avec  $\dim V := k \geq c \cdot \log(n)$  et  $V \cap K$  est  $\varepsilon$ -euclidien.

Donnons-nous une base orthonormée  $\{v_j\}_{1 \leq j \leq k}$  de  $V$  et posons

$$\phi : \begin{array}{ccc} (V, \|\cdot\|) & \hookrightarrow & (\mathbb{R}^k, |\cdot|_k) \\ \sum_{i=1}^k x_i v_i & \mapsto & \sum_{i=1}^k x_i e_i \end{array}$$

Soit  $v \in V \cap K$  tel que  $\|v\| = 1$ , comme  $K \cap V$  est  $\varepsilon$ -euclidien on a que

$$r \leq |v|_n \leq (1 + \varepsilon)r$$

La borne supérieure est immédiate car  $K \cap V \subset r(1 + \varepsilon).(V \cap B_2^n)$ , pour la borne inférieure il suffit de remarquer que  $(V \cap K)$  est un fermé de  $V$  qui contient l'ouvert  $r.(V \cap B_2^n)$  de  $V$ , comme  $v$  est dans la frontière de  $K \cap V$  il n'est pas dans l'intérieur de  $K \cap V$  et donc dans aucun ouvert contenu dans  $V \cap K$ .

Fixons des coordonnées à  $v$  dans la base  $\{v_j\}_{1 \leq j \leq k}$ ,  $v = \sum_{i=1}^k x_i v_i$ , on a que  $|v|_n = \sqrt{\sum_{i=1}^k x_i^2}$  et donc :

$$r \leq \sqrt{\sum_{i=1}^k x_i^2} \leq (1 + \varepsilon)r$$

Mais comme  $|\phi(v)|_k = \left| \sum_{i=1}^k x_i e_i \right| = \sqrt{\sum_{i=1}^k x_i^2}$ , on a que :

$$r \leq |\phi(v)|_k \leq (1 + \varepsilon)r$$

Pour tous  $x \in V \setminus \{0\}$  on peut appliqué ce qui précède à  $\frac{x}{\|x\|}$ , en utilisant la linéarité de  $\phi$  on obtient :

$$r\|x\| \leq |\phi(x)|_k \leq (1 + \varepsilon)r\|x\|$$

(3) $\Rightarrow$ (2) Soit  $\varepsilon > 0$ , par le théorème 3 il existe  $c > 0$  tel que pour tous  $n \in \mathbb{N}$  il existe un  $k > c \cdot \log(n)$  tel que  $l_2^k$  est  $(1 + \varepsilon)$ -isomorphe à  $(\mathbb{R}^n, \|\cdot\|)$  pour n'importe quelle norme  $\|\cdot\|$  sur  $\mathbb{R}^n$ . Considérons un compact convexe symétrique  $K \subset \mathbb{R}^n$  et  $\|y\| = \inf \left\{ \lambda > 0 ; \frac{y}{\lambda} \in K \right\}$ , alors  $\exists T : l_2^k \rightarrow (\mathbb{R}^n, \|\cdot\|)$  linéaire tel que :

$$\forall x \in \mathbb{R}^k, \|x\| \leq \|Tx\| \leq (1 + \varepsilon)\|x\|$$

ceci implique immédiatement que  $T$  est injective, notons  $V = \text{Im } T$ , alors la co-restriction a  $V$  de  $T$  est bijective. Soit  $y \in \partial(K \cap V)$ , c'est à dire  $\|y\| = 1$ , on sait qu'il existe un unique  $x \in \mathbb{R}^k$  tel que  $Tx = y$ , on en déduit donc

$$\|x\| \leq 1 \leq (1 + \varepsilon)\|x\| \iff \frac{1}{1 + \varepsilon} \leq \|x\| \leq 1$$

la convexité et la symétrie centrale de  $K \cap V$  nous permet de conclure que :

$$\frac{1}{1 + \varepsilon} T(B_2^k) \subset K \cap V \subset T(B_2^k)$$



## Partie 2

### Mesures de Haar

**Définition & Théorème.** (Mesures de Haar) Soit  $(X, d)$  un espace métrique,  $G$  un groupe topologique localement compact qui agit sur  $X$  et tel que :

$$\forall x, y \in X \quad \forall g \in G, \quad d(gx, gy) = d(x, y) \quad (\star)$$

alors il existe une unique mesure à un coefficient multiplicatif près, régulière définie sur les boréliens de  $X$  qui est invariante sous l'action de  $G$ , cette mesure est appelée mesure de Haar de  $X$  (où  $G$  est sous-entendu).

Considérons  $X = S^{n-1}$  avec la distance euclidienne et  $X = O(n)$  avec la norme  $\|M\| = \sup_{|x|=1} |Mx|$  alors  $G = O(n)$  le groupe des isométries vérifie  $(\star)$  pour la multiplication matricielle sur  $S^{n-1}$  et  $O(n)$ , par le théorème précédent on peut définir sans ambiguïté  $\mu, \nu$  les mesures de Haar normalisées respectivement sur  $S^{n-1}$  et  $O(n)$ . Montrons quelques propriétés qui seront utiles par la suite.

**Lemme.** Soit  $f \in C(S^{n-1})$  et  $Y = (g_1, \dots, g_n)$  où les  $\{g_i\}_{1 \leq i \leq n}$  sont i.i.d suivant une loi normale  $\mathcal{N}(0, 1)$ , alors

$$\int_{S^{n-1}} f d\mu = \mathbb{E} \left[ f \left( \frac{Y}{|Y|} \right) \right]$$

*Démonstration.* Par unicité de la mesure de Haar, il nous suffit de montrer que pour tous  $M \in O(n)$  et  $f \in C(S^{n-1})$  :

$$\begin{aligned} \mathbb{E} \left[ f \left( \frac{MY}{|MY|} \right) \right] &= \mathbb{E} \left[ f \left( \frac{Y}{|Y|} \right) \right] \\ \mathbb{E} \left[ f \left( \frac{MY}{|MY|} \right) \right] &= \int_{\mathbb{R}^n \setminus \{0\}} f \left( \frac{My}{|y|} \right) \exp \left\{ -\frac{1}{2} |y|^2 \right\} dy_1 \dots dy_n = \int_{\mathbb{R}^n \setminus \{0\}} f \left( \frac{y}{|y|} \right) \exp \left\{ -\frac{1}{2} |M^{-1}y|^2 \right\} dy_1 \dots dy_n \end{aligned}$$

comme  $|\det M| = 1$  et  $|M^{-1}y| = |y|$ , on a :

$$\mathbb{E} \left[ f \left( \frac{MY}{|MY|} \right) \right] = \mathbb{E} \left[ f \left( \frac{Y}{|Y|} \right) \right]$$

□

**Lemme.** Soit  $A \subset S^{n-1}$  un borélien alors pour tous  $x \in S^{n-1}$

$$\nu(T \in O(n); Tx \in A) = \mu(A)$$

*Démonstration.* Soit  $M \in O(n)$  et  $x \in S^{n-1}$  alors la mesure définie par  $\omega_x(A) = \nu(T \in O(n); Tx \in A)$  vérifie

$$\omega_x(MA) = \nu(T \in O(n); M^T Tx \in A) = \nu(T \in O(n); Tx \in A) = \omega_x(A)$$

L'unicité de la mesure de Haar nous permet de conclure que  $\omega_x = \mu$  car  $\omega_x(S^{n-1}) = 1$  et en particulier  $\omega_x$  ne dépend pas de  $x$ . □

## Début de la démonstration du théorème de Dvoretzky

**Théorème 4.** Soit  $f : S^{n-1} \rightarrow \mathbb{R}$  une fonction Lipschitzienne de constante  $L > 0$ , alors

$$\mu\left\{x \in S^{n-1} ; |f(x) - \mathbb{E}[f]| > \varepsilon\right\} \leq 2e^{-\frac{\varepsilon^2 n}{2L^2}}$$

Dans cette partie on s'intéresse à démontrer le résultat suivant :

**Théorème 5.** Pour tous  $\varepsilon > 0$  il existe  $c > 0$  tel que pour tout  $n \in \mathbb{N}$  et pour toute norme  $||\cdot||$  sur  $\mathbb{R}^n$  il existe un sous-espace  $V \subset \mathbb{R}^n$  tel que :

(i)  $\dim V \geq c \cdot \left(\frac{E}{b}\right)^2 n$

(ii) Pour tous  $x \in V : (1 - \varepsilon)E|x| \leq ||x|| \leq (1 + \varepsilon)E|x|$

où  $E = \int_{S^{n-1}} ||y|| d\mu(y)$  et  $b > 0$  est le plus petit réel positif tel que  $||\cdot|| \leq b|\cdot|$ .

*Démonstration.* Soit  $1 > \delta, \theta > 0$  tel que

$$\frac{1}{1 - \theta} < 1 + \varepsilon/2 \text{ et } \frac{1 - 2\theta}{1 - \theta} > 1 - \varepsilon/2$$

$$\frac{1 + \delta}{1 - \theta} < 1 + \varepsilon \text{ et } \frac{1 - 2\theta - \delta}{1 - \theta} > 1 - \varepsilon$$

Posons  $\eta = \frac{\delta E}{b}$  et fixons  $V_0 \subset \mathbb{R}^n$  un sous-espace et  $M \subset V_0 \cap S^{n-1}$  un  $\theta$ -net, où  $\dim V_0 = k$  avec  $|M| < \frac{1}{2} e^{\frac{\eta^2 n}{2}} < \left(\frac{3}{\theta}\right)^k$ . (on justifiera l'existence d'un tel ensemble dans lemme qui suit cette démonstration)

$$\nu\left(\cap_{x \in M} \{T \in O(n) ; ||Tx|| - E| \leq b\eta\}\right) = 1 - |M| \nu(T \in O(n) ; ||Ty|| - E| > b\eta), \text{ pour un } y \in M.$$

or  $\nu(T \in O(n) ; ||Ty|| - E| > b\eta) = \mu(y \in S^{n-1} ; ||y|| - E| > b\eta) \leq 2e^{-\frac{\eta^2 n}{2}}$ , donc :

$$\nu\left(\cap_{x \in M} \{T \in O(n) ; ||Tx|| - E| \leq b\eta\}\right) \geq 1 - |M| 2e^{-\frac{\eta^2 n}{2}} > 0$$

Il existe donc  $T \in O(n)$  tel que pour tous  $x \in M$  on ait  $||Tx|| - E| \leq b\eta$ , comme  $T$  est une isométrie on a que  $N = TM$  est un  $\theta$ -net sur  $V \cap S^{n-1}$  avec  $V = TV_0$ .

Si  $x \in V \cap S^{n-1}$ , il existe  $\{y_i\} \subset N$  et  $\{\beta_i\}$  une suite avec  $|\beta_i| \leq \theta^i$  tel que  $x = y_1 + \sum_{i=2}^{\infty} \beta_i y_i$ , on a donc

$$||x|| \leq ||y_1|| + \sum_{i=2}^{\infty} \theta^i ||y_i|| \leq \sum_{i=0}^{\infty} \theta^i (b\eta + E) = \frac{1}{1 - \theta} (b\eta + E)$$

Trouvons maintenant une minoration de  $||x||$ , on a  $||x - y_1|| = \left| \sum_{i=2}^{\infty} \beta_i y_i \right| \leq \sum_{i=1}^{\infty} \theta^i ||y_i|| \leq \frac{\theta}{1 - \theta} (b\eta + E)$  et donc

$$||x|| \geq ||y_1|| - ||x - y_1|| \geq (b\eta + E) - \frac{\theta}{1 - \theta} (E + b\eta) = E \frac{1 - 2\theta}{1 - \theta} - b\eta \frac{1}{1 - \theta}$$

$$E \frac{1-2\theta}{1-\theta} - b\eta \frac{1}{1-\theta} \leq \|x\| \leq \frac{1}{1-\theta} (b\eta + E)$$

Or on a  $E \frac{1-2\theta}{1-\theta} - b\eta \frac{1}{1-\theta} = E \frac{1-2\theta-\delta}{1-\theta} > E(1-\varepsilon)$  et  $\frac{1}{1-\theta} (b\eta + E) = E \frac{1+\delta}{1-\theta} < E(1+\varepsilon)$  et donc

$$E(1-\varepsilon) \leq \|x\| \leq E(1+\varepsilon)$$

Pour  $y \in V$  il suffit de prendre  $x = \frac{y}{|y|}$  et l'on a :

$$E(1-\varepsilon)|y| \leq \|y\| \leq E(1+\varepsilon)|y|$$

Il ne nous reste plus qu'à discuter de la minoration de  $k$ , en prenant le logarithme dans  $\frac{1}{2} e^{\frac{\eta^2 n}{2}} < \left(\frac{3}{\theta}\right)^k$ , on obtient :

$$k > \frac{1}{\log(3/\theta)} \left( \frac{\delta^2 E^2}{2b^2} n - \log(2) \right)$$

*Je n'arrive pas à conclure pour la dimension, par rapport au livre de Gideon et Milman j'ai remplacé dans les notations  $\varepsilon$  par  $\eta$ ,  $\varepsilon'$  par  $\delta$ ,  $\delta$  par  $\varepsilon$*  □

**Lemme.** Pour tous  $0 < \varepsilon < 1$  il existe un  $\varepsilon$ -net sur  $S^{k-1}$  de cardinal inférieur à  $\left(\frac{3}{\varepsilon}\right)^k$ .

*Démonstration.* Soit  $N = \{x_i\}_{i=1,\dots,m}$  un sous ensemble de  $S^{k-1}$  maximal pour la propriété :  $x, y \in N$ ,  $|x - y| \geq \varepsilon$ , c'est à dire pour tous  $x \in S^{k-1} \setminus N$  il existe  $i \leq m$  tel que  $|x - x_i| < \varepsilon$ , donc  $N$  est un  $\varepsilon$ -net. Les boules de centre  $x_i$  et de rayon  $\varepsilon/2$  sont donc disjointes deux à deux et toutes contenues dans  $B(0, 1 + \frac{\varepsilon}{2})$  d'où :

$$m \text{Vol}(B(x_1, \frac{\varepsilon}{2})) = \sum_{i=1}^m \text{Vol}(B(x_i, \frac{\varepsilon}{2})) = \text{Vol}(\cup_{1 \leq i \leq m} B(x_i, \frac{\varepsilon}{2})) \leq \text{Vol}(B(0, 1 + \frac{\varepsilon}{2}))$$

$$m \leq \frac{\text{Vol}(B(0, 1 + \frac{\varepsilon}{2}))}{\text{Vol}(B(x_1, \frac{\varepsilon}{2}))} = \left( \frac{1 + \frac{\varepsilon}{2}}{\frac{\varepsilon}{2}} \right)^k = \left( 1 + \frac{2}{\varepsilon} \right)^k \leq \left( \frac{3}{\varepsilon} \right)^k$$

□



## Partie 3

### Estimation de la borne inférieure du maximum d'un vecteur gaussien

Dans la suite pour estimer  $E$  nous aurons besoin d'une minoration de  $\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right]$  pour des  $g_i$  i.i.d suivant  $\mathcal{N}(0, 1)$ , nous démontrons une telle borne dans cette section.

**Lemme.** (ratio de Mill) Soit  $g$  une variable aléatoire suivant une loi  $\mathcal{N}(0, 1)$ , alors

$$\mathbb{P}(g > t) \geq \exp\left(-\frac{t^2}{2}\right) \frac{1}{\sqrt{2\pi}t + 2}$$

*Démonstration.*

□

**Théorème 6.**  $\exists A, B > 0$  tel que pour tout  $N > 1$ , et  $(g_1, \dots, g_N)$  des variables aléatoires i.i.d suivant une loi  $\mathcal{N}(0, 1)$ , on est :

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq A\sqrt{\log N} - B$$

*Démonstration.* Fixons ces notations :

(i)  $C(N) = \sqrt{2 - \frac{2 \log \log N}{\log N}}$

(ii)  $\beta_N = C(N)\sqrt{\log N}$

(iii)  $A = \cup_{i \leq N} \{X_i \geq \beta_N\}$

La démonstration va reposer sur l'égalité suivante :

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] = \mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A \right] \mathbb{P}(A) + \mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A^c \right] \mathbb{P}(A^c) \quad (\star)$$

Dans un premier temps, on s'intéresse à minorer la partie  $\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A^c \right]$ .

$$\begin{aligned} \mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A^c \right] &\geq \mathbb{E} \left[ g_1 | A^c \right] = \frac{1}{\mathbb{P}(A^c)} \int_{\mathbb{R}^N} x_1 \mathbb{1}_{A^c}(x_1, \dots, x_N) \prod_{i=1}^N \frac{\exp\left(-\frac{1}{2}x_i^2\right)}{\sqrt{2\pi}} dx_1 \dots dx_N \\ \mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A^c \right] &\geq \frac{1}{\mathbb{P}(g_1 \leq \beta_N)^N} \left( \int_{\mathbb{R}} \frac{\exp\left(-\frac{1}{2}x^2\right)}{\sqrt{2\pi}} \mathbb{1}_{\{g_1 \leq \beta_N\}} dx \right)^{N-1} \int_{-\infty}^{\beta_N} x \exp\left(-\frac{1}{2}x^2\right) \frac{dx}{\sqrt{2\pi}} \\ \mathbb{E} \left[ \max_{1 \leq i \leq N} g_i | A^c \right] &\geq \frac{1}{\mathbb{P}(g_1 \leq 0)} \int_{-\infty}^0 x \exp\left(-\frac{1}{2}x^2\right) \frac{dx}{\sqrt{2\pi}} = -\sqrt{\frac{2}{\pi}} \end{aligned}$$

En substituant dans  $(\star)$  :

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq \beta_N \mathbb{P}(A) - \sqrt{\frac{2}{\pi}} (1 - \mathbb{P}(A)) = \left( \beta_N + \sqrt{\frac{2}{\pi}} \right) \mathbb{P}(A) - \sqrt{\frac{2}{\pi}}$$

On s'intéresse maintenant a minoré  $\mathbb{P}(A)$ .

$$\mathbb{P}(A) = 1 - \mathbb{P}(A^c) = 1 - \left(1 - \mathbb{P}(g_1 > \beta_N)\right)^N$$

avec  $1 - x \leq \exp(-x)$  on a :

$$\mathbb{P}(A) \geq 1 - \exp\left(-N\mathbb{P}(g_1 > \beta_N)\right)$$

avec le ratio de Mill on obtient :

$$\mathbb{P}(A) \geq 1 - \exp\left(-N \exp\left(-\frac{\beta_N^2}{2}\right) \frac{1}{\sqrt{2\pi}\beta_N + 2}\right)$$

On peut simplifier a l'intérieur de l'exponentielle :

$$N \exp\left(-\frac{\beta_N^2}{2}\right) \frac{1}{\sqrt{2\pi}\beta_N + 2} = N^{1 - \frac{C(N)^2}{2}} \frac{1}{\sqrt{2\pi}C(N)\sqrt{\log N} + 2}$$

$$1 - \frac{C(N)^2}{2} = 1 - 1 + \frac{\log \log N}{\log N} = \frac{\log \log N}{\log N}$$

$$N^{\frac{\log \log N}{\log N}} = \exp\left(\log \log N\right) = \log N$$

$$N \exp\left(-\frac{\beta_N^2}{2}\right) \frac{1}{\sqrt{2\pi}\beta_N + 2} = \frac{\log N}{\sqrt{2\pi}C(N)\sqrt{\log N} + 2} \geq \frac{\sqrt{\log N}}{\sqrt{2\pi}C(N) + 2}$$

d'où

$$\mathbb{P}(A) \geq 1 - \exp\left(-\frac{\sqrt{\log N}}{\sqrt{2\pi}C(N) + 2}\right)$$

**Lemme.** Pour  $N \geq 2$  on a  $C(N) \leq C =: C(2) \approx 1,749$

*Démonstration.*  $C'(x) = \frac{1 - \log \log x}{2x C(x) \log(x)^2}$ , donc  $C'(x) = 0$  si et seulement si  $x = e^e$ , si  $x < e^e$  alors  $C'(x) < 0$  et si  $x > e^e$  alors  $C'(x) > 0$ , de plus

$$\lim_{x \rightarrow +\infty} C(x) = \lim_{x \rightarrow \infty} \sqrt{2 - \frac{2 \log \log x}{\log x}} = \sqrt{2}$$

Comme  $C > \sqrt{2}$  on a  $C(x) \leq C$  pour tous  $x \geq 2$ . □

Par le lemme on a donc

$$\mathbb{P}(A) \geq 1 - \exp\left(-K\sqrt{\log N}\right), \text{ avec } K = \frac{1}{\sqrt{2\pi}C + 2} \approx 0.157.$$

On injecte finalement dans  $\mathbb{E}[\max_{1 \leq i \leq N} g_i]$

$$\mathbb{E}\left[\max_{1 \leq i \leq N} g_i\right] \geq \left(\beta_N + \sqrt{\frac{2}{\pi}}\right)(1 - \exp(-K\sqrt{\log N})) - \sqrt{\frac{2}{\pi}}$$

$$\mathbb{E}\left[\max_{1 \leq i \leq N} g_i\right] \geq \left(\sqrt{2 \log N - 2 \log \log N} + \sqrt{\frac{2}{\pi}}\right)(1 - \exp(-K\sqrt{\log N})) - \sqrt{\frac{2}{\pi}}$$



Pour  $x \geq 2$  on a  $\exp(-K\sqrt{\log x}) \leq \exp(-K\sqrt{\log 2})$ , en effet comme

$$(\exp(-K\sqrt{\log x}))' = -\frac{K}{2\sqrt{\log x}} \exp(-K\sqrt{\log x}) < 0$$

par la suite posons  $a =: 1 - \exp(-K\sqrt{\log 2}) \approx 0,123$

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq (\sqrt{2 \log N - 2 \log \log N} + \sqrt{\frac{2}{\pi}})a - \sqrt{\frac{2}{\pi}}$$

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq a\sqrt{2 \log N - 2 \log \log N} - \sqrt{\frac{2}{\pi}}(1-a)$$

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq aC(N)\sqrt{\log N} - \sqrt{\frac{2}{\pi}}(1-a)$$

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq aC(e^e)\sqrt{\log N} - \sqrt{\frac{2}{\pi}}(1-a)$$

posons finalement  $A = aC(e^e) \approx 0.138$  et  $B = \sqrt{\frac{2}{\pi}}(1-a) \approx 0,699$  alors on a :

$$\mathbb{E} \left[ \max_{1 \leq i \leq N} g_i \right] \geq A\sqrt{\log N} - B$$

□

## Estimation de E

Par la suite on fixe  $\|\cdot\|$  une norme sur  $\mathbb{R}^n$ ,  $K = \text{Adh}(B_{\|\cdot\|})$  tel que  $B_2^n$  soit l'ellipsoïde de volume maximale incluse dans  $K$ , on a donc  $b = 1$ . Dans cette partie nous allons donner une estimation de  $E$ .

**Définition.** Un ellipsoïde  $D$  de  $\mathbb{R}^n$  est l'image de la boule unité euclidienne par un élément de  $GL(n)$ .

Admettons le théorème suivant de Fritz John (1910-1994) :

**Théorème 7.** (Ellipsoïde de John) Tous compact convexe symétrique d'intérieur non vide contient un unique ellipsoïde de volume maximale.

**Lemme.** (Dvoretzky-Rogers) Il existe une base orthonormée  $\{x_i\}_{i=1,\dots,n}$  tel que

$$\forall 1 \leq i \leq n, \quad e^{-1} \left(1 - \frac{i-1}{n}\right) \leq \|x_i\| \leq 1$$

*Démonstration.*  $S^{n-1}$  est compact et  $\|\cdot\|$  continue, on peut donc prendre un  $x_1 \in S^{n-1}$  qui maximise  $\|\cdot\|$  c'est à dire  $\|x_1\| = 1$ , supposons que l'on ait  $x_1, \dots, x_{k-1}$  avec  $k \leq n$  tel que pour tous  $1 \leq i \leq k-1$ ,  $x_i$  maximise  $\|\cdot\|$  sur  $S^{n-1} \cap_{j < i} x_j \neq \emptyset$  car les  $\{x_i\}_{i=1,\dots,k-1}$  sont orthogonaux deux à deux et est compact, on peut donc répéter le procédé pour trouver

$x_k$  qui maximise  $S^{n-1} \cap_{j < k} x_j$ , par récurrence on peut donc avoir  $n$  vecteurs avec ses propriétés. Fixons  $1 \leq k \leq n$ ,  $a, b \in \mathbb{R}^*$  et définissons :

$$\mathcal{E} = \left\{ \sum_{i=1}^n a_i x_i ; \sum_{i=1}^{k-1} \left( \frac{a_i}{a} \right)^2 + \sum_{i=k}^n \left( \frac{b_i}{b} \right)^2 \leq 1 \right\}$$

Supposons  $\sum_{i=1}^n a_i x_i \in \mathcal{E}$ , alors  $\sum_{i=1}^{k-1} a_i x_i \in aB_2^n$  et donc  $\|\sum_{i=1}^{k-1} a_i x_i\| \leq a$ . Si  $x \in \text{Vect}(x_k, \dots, x_n) \cap B_2^n$  on a  $\|x\| \leq \|x_k\|$  par construction, et donc  $\sum_{i=k}^n a_i x_i \in bB_2^n \Rightarrow \|\sum_{i=k}^n a_i x_i\| \leq b\|x_k\|$ , ce qui nous donne la majoration suivante

$$\left\| \sum_{i=1}^n a_i x_i \right\| \leq \left\| \sum_{i=1}^{k-1} a_i x_i \right\| + \left\| \sum_{i=k}^n a_i x_i \right\| \leq a + b\|x_k\|$$

Posons  $\phi \in GL(n)$  défini par  $\phi(\sum_{i=1}^n a_i x_i) = \sum_{i=1}^{k-1} a a_i x_i + \sum_{i=k}^n b a_i x_i$  on a  $\phi = \text{diag}(\overbrace{a, \dots, a}^{(k-1) \times}, \overbrace{b, \dots, b}^{(n-k+1) \times})$  et donc  $\det \phi = a^{k-1} b^{n-k+1}$  d'où :

$$\int_{\mathcal{E}} dx_1 \dots dx_n = \int_{B_2^n} \det \phi dx_1 \dots dx_n = a^{k-1} b^{n-k+1} \int_{B_2^n} dx_1 \dots dx_n$$

On prend  $a + b\|x_k\| = 1$  de sorte que  $\mathcal{E} \subset K$ , comme  $B_2^n$  est l'ellipsoïde de volume maximale incluse dans  $K$ , on a que

$$1 \geq \frac{\int_{\mathcal{E}} dx_1 \dots dx_n}{\int_{B_2^n} dx_1 \dots dx_n} = a^{k-1} b^{n-k+1}$$

Fixons donc pour  $k \geq 2$ ,  $b = \frac{1-a}{\|x_k\|}$  et  $a = \frac{k-1}{n}$ , en remplaçant dans l'inégalité on obtient :

$$1 \geq a^{k-1} \left( \frac{1-a}{\|x_k\|} \right)^{n-k+1} \iff \|x_k\| \geq a^{\frac{k-1}{n-k+1}} (1-a) = \left( \frac{k-1}{n} \right)^{\frac{k-1}{n-k+1}} \left( 1 - \frac{k-1}{n} \right)$$

et  $\log a^{\frac{k-1}{n-k+1}} = \frac{k-1}{n-k+1} \log \left( \frac{k-1}{n} \right) > -1$ . □

**Proposition.** (Estimation de  $E$ ) Il existe  $c = c(\varepsilon) > 0$  tel que  $E \geq c \sqrt{\frac{\log n}{n}}$ .

*Démonstration.* Par le lemme de Dvoretzky-Rogers il existe une base orthonormée  $x_1, \dots, x_n$  tel que pour  $1 \leq i \leq [n/2]$ ,  $\|x_i\| \geq e^{-1} \left( 1 - \frac{n/2-1}{n} \right) = e^{-1} \left( \frac{1}{2} + \frac{1}{n} \right) \geq (2e)^{-1}$ . Comme  $\mu$  est invariante par composition par une transformation orthogonale on a que

$$E =: \int_{S^{n-1}} \left\| \sum_{i=1}^n a_i x_i \right\| d\mu(a) = \int_{S^{n-1}} \left\| \sum_{i=1}^{n-1} a_i x_i - a_n x_n \right\| d\mu(a)$$

et donc

$$\begin{aligned} \int_{S^{n-1}} \left\| \sum_{i=1}^n a_i x_i \right\| d\mu(a) &= \frac{1}{2} \int_{S^{n-1}} \left\| \sum_{i=1}^n a_i x_i \right\| d\mu(a) + \frac{1}{2} \int_{S^{n-1}} \left\| \sum_{i=1}^{n-1} a_i x_i - a_n x_n \right\| d\mu(a) \\ \int_{S^{n-1}} \left\| \sum_{i=1}^n a_i x_i \right\| d\mu(a) &\geq \frac{1}{2} \int_{S^{n-1}} 2 \max \left\{ \left\| \sum_{i=1}^{n-1} a_i x_i \right\|, \|a_n x_n\| \right\} d\mu(a) \geq \dots \geq \int_{S^{n-1}} \max_{1 \leq i \leq n} \{ |a_i| \|x_i\| \} d\mu(a) \\ \int_{S^{n-1}} \left\| \sum_{i=1}^n a_i x_i \right\| d\mu(a) &\geq \int_{S^{n-1}} \max_{1 \leq i \leq [n/2]} \{ |a_i| \|x_i\| \} d\mu(a) \geq (2e)^{-1} \int_{S^{n-1}} \max_{1 \leq i \leq [n/2]} |a_i| d\mu(a) \end{aligned}$$

Soit  $(g_1, \dots, g_n)$ , des variables aléatoire i.i.d de loi  $\mathcal{N}(0, 1)$  alors

$$\int_{S^{n-1}} \max_{1 \leq i \leq \lfloor n/2 \rfloor} |a_i| d\mu(a) = \mathbb{E} \left[ \left( \sum_{i=1}^n g_i^2 \right)^{-\frac{1}{2}} \max_{1 \leq i \leq \lfloor n/2 \rfloor} |g_i| \right]$$

**Lemme.**  $(\sum_{i=1}^n g_i^2)^{\frac{1}{2}}(g_1, \dots, g_n)$  et  $(\sum_{i=1}^n g_i^2)^{-\frac{1}{2}}$  sont indépendants.

*Démonstration du lemme.*

□

Par le lemme on a donc

$$\mathbb{E} \left[ \left( \sum_{i=1}^n g_i^2 \right)^{-\frac{1}{2}} \max_{1 \leq i \leq \lfloor n/2 \rfloor} |g_i| \right] \cdot \mathbb{E} \left[ \left( \sum_{i=1}^n g_i^2 \right)^{\frac{1}{2}} \right] = \mathbb{E} \left[ \max_{1 \leq i \leq \lfloor n/2 \rfloor} |g_i| \right]$$

la fonction racine carré est concave, par l'inégalité de Jensen on a donc :

$$\mathbb{E} \left[ \left( \sum_{i=1}^n g_i^2 \right)^{\frac{1}{2}} \right] \leq \mathbb{E} \left[ \sum_{i=1}^n g_i^2 \right]^{\frac{1}{2}} = \sqrt{n} \mathbb{E}[g_1^2]^{\frac{1}{2}} = \sqrt{n}$$

Et finalement par le théorème 6 :

$$E \geq \frac{1}{2e\sqrt{n}} \mathbb{E} \left[ \max_{1 \leq i \leq \lfloor n/2 \rfloor} |g_i| \right] \geq \frac{A\sqrt{\log(n/2)} - B}{2e\sqrt{n}}$$

□