À rendre pour le jeudi 13 janvier

Notations :

- Si x est un nombre réel on note $[x]$ sa partie entière, c'est-à-dire le plus grand entier relatif qui est inférieur ou égal à x.
- On appelle cardinal de l'ensemble fini E le nombre de ses éléments, que l'on note $|E|$.
- On note $\mathcal{P}(E)$ l'ensemble des parties de l'ensemble E.
- Dans tout le problème on identifiera $\mathbb{R}^n$ à l'espace des matrices lignes $\mathcal{M}_{1,n}(\mathbb{R})$ et on notera $\langle x, y\rangle$ le produit scalaire canonique de ces vecteurs, soit

$$\langle x, y\rangle = \sum_{j=1}^{n} x_j y_j,$$

  les x_j, y_j étant les composantes de x et y respectivement.
- Si $\mathcal{V}$ est un sous-ensemble de $\mathbb{R}^n$ on note $\mathrm{Vect}(\mathcal{V})$ l'espace vectoriel engendré par $\mathcal{V}$. On note $\mathcal{V}^\perp$ l'orthogonal de $\mathcal{V}$, c'est-à-dire l'ensemble des vecteurs y tels que $\forall x \in \mathcal{V}$, $\langle x, y\rangle = 0$.
- Si M est une matrice carrée de nombres réels, on note $\det(M)$ son déterminant.

Dans tout le problème on pourra utiliser librement la formule de Stirling que l'on rappelle :

$$n! \underset{n\to+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Définition 1 ***(Espace de Rademacher)*** *Si $n, q \in \mathbb{N}^*$, on note*

$$\Omega_{q,n} = \{\omega = (\omega_{i,j},\ 1 \le i \le q,\ 1 \le j \le n) \text{ tels que } : \forall (i,j) \in [\![1,q]\!] \times [\![1,n]\!],\ \omega_{i,j} = \pm 1\}.$$

Pour tout $i \in \{1,\dots,q\}$ et $j \in \{1,\dots,n\}$, on introduit la variable aléatoire $M_{i,j}$ telle que

$$M_{i,j} : \left\{ \begin{array}{ccc} \Omega_{q,n} & \to & \{-1,1\} \\ \omega & \mapsto & \omega_{i,j} \end{array} \right. .$$

On munit $\Omega_{q,n}$ de la probabilité uniforme P. Cela signifie que les variables $(M_{i,j},\ 1 \le i \le q,\ 1 \le j \le n)$ sont indépendantes et de même loi :

$$P(M_{i,j} = 1) = \frac{1}{2} = P(M_{i,j} = -1).$$

Si $q = n$, on note $M^{(n)}$ la matrice aléatoire

$$M^{(n)} = \begin{pmatrix} M_{1,1} & \cdots & M_{1,n} \\ \vdots & & \vdots \\ M_{n,1} & \cdots & M_{n,n} \end{pmatrix}.$$

On note $L_1^{(n)}, \dots, L_n^{(n)}$ les vecteurs lignes de $M^{(n)}$. Par construction, ce sont des vecteurs aléatoires indépendants et de même loi.

Le but du problème est de démontrer, qu'ainsi construite, une matrice aléatoire est inversible avec forte probabilité quand n est grand :

Théorème 1 ***(Komlós)*** $\lim\limits_{n\to+\infty} P(\det(M^{(n)}) = 0) = 0.$

A Procédé de construction de matrices aléatoires à coefficients dans $\{-1,1\}$

Soit $p \in]0,1[$. On définit une suite (A_k) de matrices aléatoires d'ordre n à coefficients dans $\{-1,1\}$ selon le procédé suivant :

- on note A_0 la matrice réelle d'ordre n dont tous les coefficients sont égaux à 1 ;
- pour tout entier naturel k, on construit la matrice A_{k+1} à partir de la matrice A_k en conservant chaque coefficient de A_k égal à -1 et en changeant en -1 avec la probabilité p chaque coefficient de A_k égal à 1. Chaque coefficient égal à 1 a donc la probabilité $q = 1-p$ de ne pas être modifié ;
- le processus s'arrête quand la matrice obtenue est égale à $-A_0$.

On suppose avoir utilisé l'instruction

```
import numpy as np, numpy.random as rd
```

pour charger les bibliothèques `numpy` et `numpy.random`. Voici quelques fonctions de ces bibliothèques qui peuvent être utiles dans cette partie :

- `np.ones((n,n))` crée un tableau `numpy` de taille $n \times n$ dont tous les éléments valent 1 ;
- `A.shape` est un tuple qui contient les dimensions du tableau `A` ;
- `A.size` donne le nombre total d'éléments du tableau `A` ;
- `A.sum()` renvoie la somme de tous les éléments du tableau `A` ;
- `rd.binomial(1, p)` simule une variable aléatoire suivant la loi de Bernoulli de paramètre p.

1. Écrire en PYTHON une fonction `modifie_matrice(p, A)` qui prend en argument une probabilité p et un tableau `numpy` représentant une matrice A de $\mathcal{M}_n(\mathbb{R})$ à coefficients dans $\{-1,1\}$. Cette fonction modifie le tableau a selon le procédé décrit ci-dessus.

2. En utilisant la fonction précédente, écrire en PYTHON une fonction `nb_tours(p, n)` qui prend en argument une probabilité p et l'ordre n des matrices A_k et renvoie le plus petit entier k tel que $A_k = -A_0$, en partant de la matrice A_0.

3. Écrire en PYTHON une fonction `moyenne_tours(p, n, nbe)` qui prend en argument une probabilité p, l'ordre n des matrices A_k et un nombre entier `nbe` et qui renvoie la moyenne, sur `nbe` essais effectués, du nombre d'étapes nécessaires pour passer de A_0 à $-A_0$.

B Coefficients binomiaux

4. Soit $n \in \mathbb{N}^*$: montrer que l'application

$$k \mapsto \binom{n}{k}$$

est croissante sur $\{0, \ldots, [n/2]\}$. En déduire que pour tout $k \in \{0, \ldots, n\}$,

$$\binom{n}{k} \leq \binom{n}{[n/2]}.$$

5. Trouver un équivalent de $\binom{n}{[n/2]}$ quand n tend vers l'infini. En déduire qu'il existe un entier n_0 tel que pour $n \geq n_0$,

$$\binom{n}{[n/2]} \leq \frac{2^n}{\sqrt{n}}. \qquad (1)$$

6. Montrer que pour tout entier non nul n et tout $k \in \{0, \ldots, n\}$,

$$\binom{n}{k} 2^{k-1} \leq n^k.$$

On note $(e_i,\ 1 \leq i \leq n)$ la base canonique de $\mathbb{R}^n$ et $v = \sum_{i=1}^{n} e_i$. On identifie $\Omega_{1,n}$ et le sous-ensemble de $\mathbb{R}^n$

$$\left\{\sum_{i=1}^n \omega_i e_i,\ (\omega_1, \ldots, \omega_n) \in \Omega_{1,n}\right\}.$$

7. Pour tout $i \in \{1, \ldots, n\}$, exprimer e_i en fonction de v et $v - 2e_i$. En déduire que $\mathrm{Vect}(\Omega_{1,n}) = \mathbb{R}^n$.

C Dimension 2

8. Déterminer l'espérance de $\det M^{(2)}$.

9. Montrer que la variance de $\det M^{(2)}$ est égale à 2.

10. Calculer $P(\det M^{(2)} = 0)$.

D Quelques bornes

On suppose dorénavant $n \geq 2$.

11. Quelle est la probabilité que les deux premières lignes de $M^{(n)}$ soit égales ou opposées ?
En déduire que $P\left(\det M^{(n)} = 0\right) \geq 2^{1-n}$ si $n \geq 2$.

12. Soient $l_1, \ldots, l_n$ des vecteurs non nuls de $\mathbb{R}^n$. Montrer que ces vecteurs sont liés si et seulement si, il existe $j \in \{1, \ldots, n-1\}$ tel que

$$l_{j+1} \in \mathrm{Vect}(\{l_1, \cdots, l_j\}).$$

En déduire que

$$P(\det M^{(n)} = 0) \leq \sum_{j=1}^{n-1} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)}\right). \qquad (2)$$

Soit $\mathcal{H}$ un sous-espace vectoriel de $\mathbb{R}^n$ de dimension d. On rappelle que $\mathcal{H}^\perp$ est un sous-espace vectoriel de dimension $n-d$ et que $(\mathcal{H}^\perp)^\perp = \mathcal{H}$.

13. Montrer alors qu'il existe des réels $(\alpha_{i,j},\ 1 \leq i \leq n-d,\ 1 \leq j \leq n)$ tels que

$$x = (x_1, \ldots, x_n) \in \mathcal{H} \Leftrightarrow \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n-d,1} & \cdots & \alpha_{n-d,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

14. Montrer qu'il existe $1 \leq i_1 < \cdots < i_d \leq n$ tel que pour tout $(y_1, \ldots, y_d) \in \mathbb{R}^d$ il existe un unique $x = (x_1, \ldots, x_n) \in \mathcal{H}$ tel que $x_{i_k} = y_k$ pour $k = 1, \ldots, d$.

15. En déduire que

$$P(L_1^{(n)} \in \mathcal{H}) \leq 2^{d-n},$$

puis que pour tout $j \in \{1, \ldots, n-1\}$,

$$P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) \leq 2^{j-n} \qquad (3)$$

Indication : on pourra utiliser la conséquence suivante de la formule des probabilités totales

$$P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) = \sum_{l_1, \ldots, l_j \in \Omega_{1,n}} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)}) | L_1^{(n)} = l_1, \ldots, L_j^{(n)} = l_j\right) \times P\left(L_1^{(n)} = l_1, \ldots, L_j^{(n)} = l_j\right)$$

et l'indépendance des vecteurs lignes. Soit $q < n$ et $\omega \in \Omega_{q,n}$. On note $l_1, \cdots, l_q$ ses vecteurs lignes.

16. Montrer que l'on peut trouver un vecteur non nul orthogonal à $\mathrm{Vect}(l_i,\ i = 1, \ldots, q)$ qui soit à coordonnées dans $\mathbb{Z}$.

E Théorème de Erdös-Littlewood-Offord

Définition 2 *Soit n un entier non nul. Soit $\mathcal{A}$ un sous-ensemble de $\mathcal{P}(\{1,\dots,n\})$. On dit que $\mathcal{A}$ est une anti-chaîne si deux éléments distincts A et B quelconques de $\mathcal{A}$ sont incomparables, c'est-à-dire tels que A n'est pas inclus dans B et B n'est pas inclus dans A.*

Commençons par un exemple. Soit $k \in \{1,\dots,n\}$ et $\mathcal{A}_k$ l'ensemble des parties de $\{1,\dots,n\}$ de cardinal k.

17. Montrer que $\mathcal{A}_k$ est une anti-chaîne et que

$$|\mathcal{A}_k| \leq \binom{n}{[n/2]} \leq \frac{2^n}{\sqrt{n}},$$

la deuxième inégalité ayant lieu pour n assez grand.

Définition 3 *Soit $\mathcal{A}$ une anti-chaîne et $A \in \mathcal{A}$, de cardinal noté $|A|$. On note S_A, l'ensemble des bijections σ de $\{1,\dots,n\}$ dans lui-même telles que la restriction de σ à $\{1,\dots,|A|\}$ soit une bijection de $\{1,\dots,|A|\}$ dans A.*

18. Quel est le cardinal de S_A ?

19. Soit $B \in \mathcal{A}$ avec $B \neq A$. Montrer que $S_A \cap S_B = \emptyset$.

20. En déduire que si a_k désigne, pour $k \leq n$, le nombre d'éléments de $\mathcal{A}$ de cardinal k, alors

$$\sum_{k=0}^{n} \frac{a_k}{\binom{n}{k}} \leq 1.$$

21. Montrer que

$$|\mathcal{A}| \leq \binom{n}{[n/2]}.$$

Soit $v = (v_1,\dots,v_n) \in \mathbb{R}^n$ tel que $v_j \geq 1$ pour tout $j = 1,\dots,n$. Si $A \subset \{1,\dots,n\}$ on pose

$$s_A = \sum_{j\in A} v_j - \sum_{j\in A^c} v_j$$

où A^c est le complémentaire de A dans $\{1,\dots,n\}$.

22. Montrer que si $A \subset B \subset \{1,\dots,n\}$, $A \neq B$, alors

$$s_B - s_A \geq 2.$$

23. Soit J un intervalle ouvert de $\mathbb{R}$ de longueur 2 : montrer que si n est assez grand alors

$$P(\langle L_1^{(n)}, v\rangle \in J) \leq \frac{1}{\sqrt{n}}.$$

Montrer que cette propriété reste vraie si l'on suppose seulement que pour tout $j \in \{1,\dots,n\}$, $|v_j| \geq 1$. *Indication : construire une bijection entre $\Omega_{1,n}$ et l'ensemble des parties de $\{1,\dots,n\}$. Construire une anti-chaîne intéressante.*

F Universalité

Dans tout ce qui suit, k est un entier inférieur à n.

Définition 4 *Soit $\mathcal{V} \subset \Omega_{1,n}$. L'ensemble $\mathcal{V}$ est dit k-universel si pour tous les k-uplets $1 \leq j_1 < j_2 \cdots < j_k \leq n$ et tout $\omega \in \Omega_{1,n}$, il existe $v \in \mathcal{V}$ tel que*

$$v_{j_m} = \omega_{1,j_m}, \text{ pour tout } m = 1, \ldots, k.$$

24. Soit $d \in \{1, \ldots, n\}$. Montrer l'inclusion

$$\left\{\{L_1^{(n)}, \ldots, L_d^{(n)}\} \text{ non } k\text{-universel}\right\} \subset \bigcup_{\substack{(j_1,\ldots,j_k)\in\{1,\ldots,n\}^k \\ j_1<\cdots<j_k}} \bigcup_{\omega\in\Omega_{1,k}} \bigcap_{i=1}^{d} \bigcup_{m=1}^{k} \{M_{i,j_m} \neq \omega_{1,j_m}\}.$$

(On rappelle que $L_i^{(n)} = (M_{i,1}, \ldots, M_{i,n})$).

25. Montrer que la probabilité que $\{L_1^{(n)}, \ldots, L_d^{(n)}\}$ ne soit pas k-universel est majorée par

$$\binom{n}{k} 2^k (1 - 2^{-k})^d.$$

26. En déduire que si $d \geq n/2$ et $k \leq \ln n$, alors, pour n assez grand,

$$P\left(\{L_1^{(n)}, \ldots, L_d^{(n)} \text{ non } k\text{-universel}\right) \leq \frac{1}{n}. \qquad (4)$$

27. Soit $\mathcal{V} \subset \Omega_{1,n}$ un ensemble k-universel tel qu'il existe $v \in \mathcal{V}^{\perp} \setminus \{0\}$: montrer que v a au moins $k+1$ coordonnées non nulles. En vertu de la question 16, on peut supposer que les coordonnées de v sont des entiers relatifs.

28. Montrer que si k est assez grand

$$P\left(L_1^{(n)} \in \mathrm{Vect}(\mathcal{V})\right) \leq P(\langle L_1^{(n)}, v\rangle = 0) \leq k^{-1/2}. \qquad (5)$$

Soit $(t_n, n \in \mathbb{N})$ une suite croissante d'entiers telle que $t_n/n \to 0$.

29. Montrer que si n est assez grand alors $n - t_n \geq n/2$ et

$$\sum_{j=n-t_n+1}^{n-1} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) \leq \frac{2t_n}{\sqrt{\ln n}}. \qquad (6)$$

Indication : on distinguera les cas selon que $\mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})$ *est k-universel ou pas et l'on prendra $k = [\ln n]$.*

G Théorème de Komlós

30. En déduire le théorème de Komlós.
Indication : on pourra partir de (2) *et choisir convenablement une suite* $(t_n,\ n \geq 1)$.