PSI* 2023/24 DL 1

Théorème de Komlós

Instructions et objectifs

Je suis parti d'un sujet de concours qui utilise uniquement le cours de Sup. Il utilise des moyens "élémentaires" mais de façon assez technique. Les parties A et B sont relativement accessibles. Ensuite, les parties C,D commencent de façon parfois un peu déconcertante mais pas vraiment difficile et terminent par des questions bien plus ardues. La partie E demande de ne pas se laisser impressionner par les notations, et de repérer des choses faisables malgré tout, ce qui est une aptitude à travailler.

Pour aborder ce sujet vous pouvez relire rapidement le cours sur les variables aléatoires, notamment les propriétés sur espérance et variance des sommes et produits de variables aléatoires, indépendantes ou non. Je rappelle simplement le résultat suivant :

Propriété 1. Lemme de coalition

Si $(X_1, \ldots, X_p, X_{p+1}, \ldots, X_n)$ sont des variables aléatoires indépendantes, alors pour toutes fonctions f et g, $U = f(X_1, \ldots, X_p)$ et $V = g(X_{p+1}, \ldots, X_n)$ sont indépendantes.

Exemple : si (X, Y, Z, T) sont des v.a. indépendantes alors $X + Y$ et ZT^2 sont indépendantes.

Travail demandé : essayez de traiter sans attendre les parties A et B. Vous pouvez réfléchir à C et D de façon séparée et aller aussi loin que vous pouvez dans chacune. Les questions E et F sont pour qui veut. *N'hésitez pas à demander des indications, d'où l'importance de commencer à chercher sans tarder.*

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 *(oui normalement c'est* $\lfloor x \rfloor$ *mais ils ne maîtrisent pas tous les codes* LaTeX *on dirait).*

— 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 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 *(elle fera bientôt partie du cours en effet)* :

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

Déf - Espace de Rademacher

Si $n, q \in \mathbb{N}^*$, on note

$$\Omega_{q,n} = \{\omega = (\omega_{i,j},\ 1 \le i \le q,\ 1 \le j \le n) \text{ tels que } \omega_{i,j} = \pm 1, \forall i, j\}.$$

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

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

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

$$\lim_{n\to+\infty} P(\det(M^{(n)}) = 0) = 0.$$

A Premiers résultats

1. Déterminer l'espérance de $\det M^{(2)}$.
2. Montrer que la variance de $\det M^{(2)}$ est égale à 2.
3. Calculer $P(\det M^{(2)} = 0)$.

   - On suppose dorénavant $n \ge 2$. Il existe au programme de MPSI une formule donnant le déterminant en fonction des composantes de M. Cette formule est hors programme PCSI/PSI et il vaut mieux l'éviter. Elle peut d'ailleurs être délicate à manier et est en fait rarement nécessaire. Ici, vous procéderez à des démonstrations par récurrence.

4. Calculer $\mathbb{E}\left[\det M^{(n)}\right]$ en fonction de n.
5. Montrer que $\mathbb{V}\left[\det M^{(n)}\right] = n!$.
6. Quelle est la probabilité que les deux premières lignes de $M^{(n)}$ soit égales ou opposées ?
   En déduire que $P\left(\det M^{(n)} = 0\right) \ge 2^{1-n}$ si $n \ge 2$.

B Coefficients binomiaux

7. 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 $k \in \{0, \ldots, n\}$,
$$\binom{n}{k} \leq \binom{n}{[n/2]}.$$

8. 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 $n \geq n_0$,
$$\binom{n}{[n/2]} \leq \frac{2^n}{\sqrt{n}}. \qquad (1)$$

9. Montrer que pour tout entier non nul n et tout $k \in \{0, \ldots, n\}$,
$$\binom{n}{k} 2^{k-1} \leq n^k.$$

C Bornes issues de l'algèbre linéaire

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

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

12. Montrer alors qu'il existe des réels $(\alpha_{i,j},\ 1 \leq i \leq n-d,\ 1 \leq j \leq n)$ tels que
$$x = (x_1, \ldots, x_n) \in \mathcal{H} \Leftrightarrow \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n-d,1} & \cdots & \alpha_{n-d,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

13. En utilisant le pivot de Gauss, 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 $k = 1, \ldots, d$. *Deux remarques stratégiques en note*[1] [2].
14. En déduire que
$$P(L_1^{(n)} \in \mathcal{H}) \leq 2^{d-n},$$

1. Dans cette question la première difficulté est de bien mettre le doigt sur ce qui est demandé pour pouvoir l'utiliser ensuite. Proposez une reformulation simple, c'est cela le point important pour pouvoir poursuivre, notamment le début de la question 14.

2. Le concepteur a choisi de demander un argument invoquant le pivot de Gauss, mais il faut réaliser que cela reste un argument théorique, sans calcul explicite puisqu'on n'a pas de valeurs concrètes ni de propriétés particulières, donc en utilisant votre connaissance du fonctionnement général de l'algorithme. On peut trouver cela assez simple, ou pas. Typiquement, le jour J, on ne s'acharne pas si ça ne vient pas, mais on y revient de temps en temps.

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.

• On verra que cette majoration est utile, mais pas suffisante.

15. Soit $q < n$ et $\omega \in \Omega_{q,n}$. On note $l_1, \cdots, l_q$ ses vecteurs lignes. En reprenant la démarche de la question 13, 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 $\mathbb{Z}$.

D Théorème de Erdös-Littlewood-Offord

Déf - Anti-chaîne

Soit n un entier non nul. Soit $\mathcal{A}$ un sous-ensemble de $\mathcal{P}(\{1, \ldots, n\})$. 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.

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

• Soit $\mathcal{A}$ une anti-chaîne de $\mathcal{P}(\{1, \ldots, n\})$. Soit $A \in \mathcal{A}$, de cardinal noté $c = |A|, (c \leq n)$. On note S_A, l'ensemble des bijections σ de $\{1, \ldots, n\}$ dans lui-même telles que la restriction de σ à $\{1, \ldots, c\}$ soit une bijection de $\{1, \ldots, c\}$ dans A.

17. Quel est le cardinal de S_A ?
18. Soit $B \in \mathcal{A}$ avec $B \neq A$. Montrer que $S_A \cap S_B = \emptyset$.
19. En déduire que si a_k désigne, pour $k \leq n$, le nombre d'éléments de $\mathcal{A}$ de cardinal k, alors

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

20. Montrer que

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

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

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

$$s_B - s_A \geq 2.$$

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

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

Indication : construire une bijection entre $\Omega_{1,n}$ et l'ensemble des parties de $\{1,\ldots,n\}$. Construire une anti-chaîne intéressante.

Montrer que cette propriété reste vraie si l'on suppose seulement que pour tout $j \in \{1,\ldots,n\}$, $|v_j| \geq 1$.

E Universalité

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

Déf - Universalité

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

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

23. Soit $d \in \{1,\ldots,n\}$. Montrer l'égalité

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

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

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

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

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

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

26. Soit $\mathcal{V} \subset \Omega_{1,n}$ un ensemble k-universel tel qu'il existe $w \in \mathcal{V}^\perp \setminus \{0\}$: montrer que w a au moins $k+1$ coordonnées non nulles.

• En vertu de la question 15, on peut supposer que les coordonnées de w sont des entiers relatifs.

27. Montrer que si k est assez grand

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

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

28. 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 $k = [\ln n]$.

F Théorème de Komlós

29. En déduire le théorème de Komlós.

Indication : on pourra partir de (2) et choisir convenablement une suite $(t_n,\ n \geq 1)$.