

Pour le corrigé, j'utiliserai la notation $M^\top$ pour la transposée (seule notation au programme depuis 2022) et non tM (ancienne notation).

Partie I

- $\mathcal{M}_n(\{-1, 1\})$ est l'ensemble des matrices carrées de taille n dont les coefficients appartiennent tous à $\{-1, 1\}$. La matrice nulle n'appartient pas à cet ensemble (la matrice I_n non plus...), donc $\mathcal{M}_n(\{-1, 1\})$ n'est pas un sev de $\mathcal{M}_n(\mathbb{R})$.
 • $\mathcal{M}_n(\{-1, 1\})$ est en bijection avec $\{-1, 1\}^{n^2}$ (les matrices de cet ensemble ont n^2 coefficients) donc

$$\text{Card}(\mathcal{M}_n(\{-1, 1\})) = 2^{n^2}.$$

- Soit $A \in \mathcal{M}_n(\{-1, 1\})$, soit $(X, Y) \in (\{-1, 1\}^n)^2$, alors en notant $(a_{i,j})_{1 \leq i,j \leq n}$ les coefficients de A , $(x_i)_{1 \leq i \leq n}$ et $(y_i)_{1 \leq i \leq n}$ les coefficients de X et de Y :

$$X^\top AY = \sum_{1 \leq i,j \leq n} a_{i,j} x_i y_j.$$

Pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$, $a_{i,j} x_i y_j \in \{-1, 1\}$ (produit de trois éléments de $\{-1, 1\}$), donc on peut utiliser l'encadrement : $-1 \leq a_{i,j} x_i y_j \leq 1$. De plus, la somme contient n^2 termes donc on obtient bien :

$$-n^2 \leq \sum_{1 \leq i,j \leq n} a_{i,j} x_i y_j = X^\top AY \leq n^2, \text{ ceci pour tout } (X, Y) \in (\{-1, 1\}^n)^2.$$

• Écrire $-1 \leq a_{i,j} x_i y_j \leq 1$ revient à $a_{i,j} x_i y_j \in \{-1, 0, 1\}$. Donc on a fait apparaître une inclusion stricte pour chaque terme (la valeur 0 n'est pas possible)...

Plus précisément, la somme $\sum_{1 \leq i,j \leq n} a_{i,j} x_i y_j$ contient n^2 termes impairs (valant tous 1 ou -1) donc le résultat de cette somme a la même parité que n^2 , donc que n ce qui permet de préciser :

$$\forall (X, Y) \in (\{-1, 1\}^n)^2, X^\top AY \in \{k \in \llbracket -n^2, n^2 \rrbracket, k \text{ de même parité que } n\} \subsetneq \llbracket -n^2, n^2 \rrbracket.$$

• Soit $k \in S(A)$, alors il existe $(X, Y) \in (\{-1, 1\}^n)^2$ tel que $X^\top AY = k$.

Or $-X = (-x_i)_{1 \leq i \leq n} \in \{-1, 1\}^n$ aussi et $(-X)^\top AY = -X^\top AY = -k$ donc $-k \in S(A)$ aussi.

- On a par hypothèse : $(A, B) \in \mathcal{M}_n(\{1, 1\})^2$, $B = CAD$ avec $C = \text{diag}(c_1, \dots, c_n)$ et $D = \text{diag}(d_1, \dots, d_n)$ où $(c_1, \dots, c_n, d_1, \dots, d_n) \in \{-1, 1\}^{2n}$.

Alors pour tout $(X, Y) \in (\{-1, 1\}^n)^2$, $X^\top BY = (CX)^\top A(DY)$ car $C^\top = C$ (matrice diagonale donc symétrique).

De plus, avec les notations précédentes : $CX = \begin{pmatrix} c_1 x_1 \\ \vdots \\ c_n x_n \end{pmatrix} = \begin{pmatrix} \pm x_1 \\ \vdots \\ \pm x_n \end{pmatrix} \in \{-1, 1\}^n$ car $X \in \{-1, 1\}^n$. Et de même, $DY \in \{-1, 1\}^n$.

Donc $X^\top BY = (X')^\top AY'$ avec $(X', Y') = (CX, DY) \in (\{-1, 1\}^n)^2$ donc $X^\top BY \in S(A)$, ceci pour tout $(X, Y) \in (\{-1, 1\}^n)^2$. Cela prouve l'inclusion $S(B) \subset S(A)$.

• Comme C et D ont leurs coefficients diagonaux tous non nuls, elles sont inversibles. Et comme leurs coefficients diagonaux sont dans $\{-1, 1\}$:

$$C^{-1} = \text{diag}\left(\frac{1}{c_1}, \dots, \frac{1}{c_n}\right) \underset{\substack{c_i = \pm 1 \\ \text{pour tout } i}}{=} \text{diag}(c_1, \dots, c_n) = C \quad \text{et de même, } D^{-1} = D.$$

Donc on peut écrire : $A = C^{-1}BD^{-1} = CBD$. D'après la première inclusion prouvée, en échangeant les rôles de A et B , on a également $S(A) \subset S(B)$ et finalement $S(A) = S(B)$.

4. • D'après 2., avec $n = 2$, $S(I)$ et $S(J)$ sont inclus dans $\{-4, -2, 0, 2, 4\}$ et symétriques. Par ailleurs, $\{-1, 1\}^2$ contient 4 éléments : $X = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $Y = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $-X$ et $-Y$. Il y a donc 16 produits envisageables pour les éléments de $S(I)$ et de $S(J)$.

• On a $X^\top IX = (-X)^\top I.(-X) = 4$ donc $4 \in S(A)$; et par symétrie, $-4 \in S(A)$ (en prenant $(-X)^\top IX$ ou $X^\top I.(-X)$).

De plus, $IY = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ donc $Z^\top IY = 0$ pour tout $Z \in \{-1, 1\}^2$. Donc $0 \in S(I)$.

De même, $Y^\top I = \begin{pmatrix} 0 & 0 \end{pmatrix}$ donc $Y^\top IZ = 0$ pour tout $Z \in \{-1, 1\}^2$. Et de même en remplaçant Y par $-Y$ (à gauche et/ou à droite du produit).

Les seuls produits ne faisant pas intervenir Y ou $-Y$ ont été vus au début, ils donnent 4 ou -4 . Et tous les produits faisant intervenir Y et/ou $-Y$ (à gauche ou à droite) donnent 0. On en déduit : $S(I) = \{-4, 0, 4\}$.

• $JX = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$ et $JY = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ donc

$$Z^\top JX \in \{-2, 2\} \text{ et } Z^\top JY \in \{-2, 2\} \text{ pour tout } Z \in \{-1, 1\}^2.$$

On en déduit que les seules valeurs possibles des 16 produits $Z^\top JZ'$ possibles, avec $(Z, Z') \in \{X, -X, Y, -Y\}$, sont 2 et -2 . Donc $S(J) = \{-2, 2\}$.

• Pour $S(A)$ avec $A \in \mathcal{M}_2(\{-1, 1\})$ quelconque, l'idée est de se ramener à I ou J par des produits à gauche et à droite par des matrices diagonales à coefficients dans $\{-1, 1\}$, et d'appliquer 3.

On sait que $\mathcal{M}_2(\{-1, 1\})$ contient $2^4 = 16$ éléments.

* Pour $A = \pm I$, on a $S(A) = S(I)$ (par symétrie de $S(I)$). Pour $A = \pm J$, $S(A) = S(J)$.

Ce cas correspond aux quatre matrices telles que $a_{1,2}$ et $a_{2,1}$ soient égaux à $a_{1,1}$.

* On remarque que $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = J$.

Donc pour $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ ou son opposé, $S(A) = S(J)$.

Et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = I$.

Donc pour $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$ ou son opposé, on a $S(A) = S(I)$.

Ce cas correspond aux quatre matrices telles que $a_{1,2} = a_{1,1} = -a_{2,1}$.

* On remarque que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = J$.

Donc pour $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ ou son opposé, $S(A) = S(J)$.

Et $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = I$.

Donc pour $A = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$ ou son opposé, on a $S(A) = S(I)$.

Ce cas correspond aux quatre matrices telles que $a_{2,1} = a_{1,1} = -a_{1,2}$.

* Enfin, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = I$.

Donc pour $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ ou son opposé, $S(A) = S(I)$.

Et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = J$.

Donc pour $A = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ ou son opposé, on a $S(A) = S(J)$.

Ce cas correspond aux quatre matrices telles que $a_{2,1} = a_{1,2} = -a_{1,1}$.

On a bien traité tous les cas, donc pour tout $A \in \mathcal{M}_2(\{-1, 1\})$, on a soit $S(A) = S(I) = \{-4, 0, 4\}$, soit $S(A) = S(J) = \{-2, 2\}$.

Je ne vois pas comment faire plus rapide, mais assez précis (sans tomber dans la facilité de "on voit bien que..." qui ne prouverait rien).

5. Remarquons que, pour $n = 2$, les trois conditions sont bien équivalentes : I est de rang 1, $4 \in S(I)$ et $I = X^\top X$ avec $X = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$; et sinon, J est de rang 2 et $4 \notin S(J)$.

On rappelle que, si $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, alors $XY^\top$ est la matrice de taille n dont les coefficients sont les $x_i y_j$, $(i, j) \in \llbracket 1, n \rrbracket^2$ (vu plusieurs fois en DM/DS/TD) ; $XY^\top$ est de rang 1 sauf si $X = Y = 0$ (sera justifié pour (b) $\Rightarrow$ (c), mais classique).

$\boxed{(a) \Rightarrow (b)}$: Supposons que $n^2 \in S(A)$, alors il existe $(X, Y) \in (\{-1, 1\}^n)^2$ tel que $X^\top AY = n^2$.

On note, comme d'habitude, $A = (a_{i,j})_{1 \leq i, j \leq n}$, $X = (x_i)_{1 \leq i \leq n}$ et $Y = (y_i)_{1 \leq i \leq n}$, alors on a

$$X^\top AY = \sum_{1 \leq i, j \leq n} a_{i,j} x_i y_j = n^2 \quad \text{et} \quad a_{i,j} x_i y_j \in \{-1, 1\} \text{ pour tout } (i, j) \in \llbracket 1, n \rrbracket^2$$

donc $\sum_{1 \leq i, j \leq n} (1 - a_{i,j} x_i y_j) = n^2 - n^2 = 0$ et c'est une somme de termes a priori positifs ou nuls.

On en déduit, pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$: $a_{i,j} x_i y_j = 1$; de plus, $x_i y_j \neq 0$ (car $x_i y_j \in \{-1, 1\}$) donc $a_{i,j} = \frac{1}{x_i y_j}$. Comme $x_i \in \{-1, 1\}$, $\frac{1}{x_i} = x_i$; et de même pour y_j . Donc

$$\forall (i, j) \in \llbracket 1, n \rrbracket^2, \quad a_{i,j} = x_i y_j = (XY^\top)_{i,j} \quad \text{donc} \quad A = XY^\top, \text{ avec } (X, Y) \in (\{-1, 1\}^n)^2.$$

$\boxed{(b) \Rightarrow (a)}$: Supposons qu'il existe $(X, Y) \in (\{-1, 1\}^n)^2$ tel que $A = XY^\top$. Alors $X^\top AY = (X^\top X)(Y^\top Y)$.

Or $X^\top X = \sum_{i=1}^n x_i^2 = n$ (car les x_i valent tous 1 ou -1), et de même pour Y . Donc

$$X^\top AY = n^2 \text{ lorsque } A = XY^\top, \text{ donc } n^2 \in S(A).$$

$\boxed{(b) \Rightarrow (c)}$: C'est la question classique. Supposons qu'il existe $(X, Y) \in (\{-1, 1\}^n)^2$ tel que $A = XY^\top$.

Alors les n colonnes de A sont respectivement $y_1 X, y_2 X, \dots, y_n X$: elles sont non nulles et toutes colinéaires à X . Donc

$$\text{Im}(A) = \text{Vect}(X) \quad \text{et} \quad \text{rg}(A) = 1$$

$\boxed{(c) \Rightarrow (b)}$: Supposons que $\text{rg}(A) = 1$, avec $A \in \mathcal{M}_n(\{-1, 1\})$ (autre implication classique, mais il faudra préciser que X et Y sont à coefficients dans $\{-1, 1\}$).

Alors toutes les colonnes de A sont colinéaires entre elles (car A est de rang 1), et plus précisément, elles sont toutes égales ou opposées à la première colonne C_1 (car les coeff de A valent 1 ou -1, donc les coefficients de proportionnalité entre les colonnes valent 1 ou -1).

Autrement dit, il existe $(\alpha_2, \dots, \alpha_n) \in \{-1, 1\}^{n-1}$ tels que $C_2 = \alpha_2 C_1, \dots, C_n = \alpha_n C_1$.

En notant $Y = \begin{pmatrix} 1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in \{-1, 1\}^n$ on a alors $A = C_1 Y^\top$, avec $(C_1, Y) \in (\{-1, 1\}^n)^2$.

6. Il y a 2^{n^2} éléments dans $\mathcal{M}_n(\{-1, 1\})$ (cf 1.), la proportion cherchée est donc $\frac{\text{Card}(E)}{2^{n^2}}$ où E est l'ensemble des $A \in \mathcal{M}_n(\{-1, 1\})$ telles que $n^2 \in S(A)$.

• D'après (a) $\Leftrightarrow$ (b), l'application $\varphi : (\{-1, 1\}^n)^2 \rightarrow E, (X, Y) \mapsto XY^\top$ est **surjective**. On voit que cette application n'est pas injective (donc pas bijective) car $(-X)(-Y)^\top = XY^\top$ pour tout (X, Y) donc tout élément de E admet au moins deux écritures comme en (b).

• Vérifions que, pour $(X, Y, X', Y') \in (\{-1, 1\}^n)^4$, $XY^\top = X'(Y')^\top \Leftrightarrow \begin{cases} (X', Y') = (X, Y) \\ \text{ou } (X', Y') = (-X, -Y) \end{cases}$.

Autrement dit, vérifions que tout élément de E admet exactement deux antécédents par φ .

Supposons donc $XY^\top = X'(Y')^\top$, alors avec des notations évidentes :

$$x_i y_j = x'_i y'_j \text{ pour tout } (i, j) \in \llbracket 1, n \rrbracket^2 \quad (*).$$

On sait que les coefficients de X et X' appartiennent à $\{-1, 1\}$ donc en particulier, $x'_1 = \pm x_1$.

* 1er cas : $x_1 = x'_1$.

D'après (*), $x_1 y_j = x'_1 y'_j$ donc $y_j = y'_j$ (car $x_1 = x'_1 \neq 0$), ceci pour tout $j \in \llbracket 1, n \rrbracket$. Donc $Y = Y'$.

Mais alors pour tout $i \in \llbracket 2, n \rrbracket$, $x_i y_1 = x'_i y'_1$, donc $x_i = x'_i$ (car en particulier on a prouvé $y_1 = y'_1$). Cela prouve que $X = X'$.

On a donc prouvé que, **dans le cas $x_1 = x'_1$, $(X', Y') = (X, Y)$.**

* 2ème cas : $x_1 = -x'_1$.

D'après (*), $x_1 y_j = x'_1 y'_j$ donc $y_j = -y'_j$ (car $x_1 \neq 0$ et $\frac{x'_1}{x_1} = -1$). Ceci pour tout $j \in \llbracket 1, n \rrbracket$. Donc $Y = -Y'$.

Mais alors pour tout $i \in \llbracket 2, n \rrbracket$, $x_i y_1 = x'_i y'_1$, donc $x_i = -x'_i$ (car en particulier on a prouvé $y_1 = -y'_1 \neq 0$). Cela prouve que $X = -X'$.

On a donc prouvé que, **dans le cas $x_1 = -x'_1$, $(X', Y') = (-X, -Y)$.**

• Ainsi, $\text{Card}(\{-1, 1\}^n) = 2\text{Card}(E)$ car tout élément de E s'écrit exactement de deux façons comme en (b) de 5. On pourrait dire également que tout élément de E admet une unique écriture $XY^\top$ telle que $x_1 = 1$, donc que E est en bijection avec $\{(X, Y) \in (\{-1, 1\}^n)^2 \mid x_1 = 1\}$.

Donc $\text{Card}(E) = \frac{\text{Card}(\{-1, 1\}^n)}{2} = \frac{(2^n)^2}{2} = 2^{2n-1}$.

• Finalement : la proportion d'éléments $A \in \mathcal{M}_n(\{-1, 1\})$ tels que $n^2 \in S(A)$ est $p = \frac{2^{2n-1}}{2^{2n}} = \frac{1}{2^{2n-2n+1}} = \frac{1}{2^{(n-1)^2}}$.

Partie II

Des idées communes avec le DM7, c'est un thème assez classique...

$U_1, \dots, U_k$ i.i.d suivant la loi $\mathcal{U}_{\{-1, 1\}}$ (Rademacher)

1. Soit $\lambda \in \mathbb{R}$, alors par la formule de transfert, $\mathbb{E}(e^{\lambda U_1}) = e^{-\lambda} \mathbb{P}(U_1 = -1) + e^{\lambda} \mathbb{P}(U_1 = 1) = \frac{e^{-\lambda} + e^{\lambda}}{2} = \text{ch}(\lambda)$.

Première preuve : Classique, l'idée est donnée dans Q5 du DM7, on utilise les développements en séries entières de $\text{ch}(\lambda)$ et $e^{\lambda^2/2}$.

Pour tout $\lambda \in \mathbb{R}$, $\text{ch}(\lambda) = \sum_{n=0}^{+\infty} \frac{\lambda^{2n}}{(2n)!}$.

Pour tout $n \in \mathbb{N}$, $(2n)! = \prod_{i=1}^{2n} i \geq \prod_{\substack{1 \leq i \leq 2n \\ i \text{ pair}}} i = \prod_{j=1}^n 2j = 2^n (n!)$.

Donc pour tout $\lambda \in \mathbb{R}$ et pour tout $n \in \mathbb{N}$, $\frac{\lambda^{2n}}{(2n)!} \leq \frac{\lambda^{2n}}{2^n (n!)} = \frac{(\lambda^2/2)^n}{n!}$ (car $\lambda^{2n} \geq 0$).

Finalement, pour tout $\lambda \in \mathbb{R}$, $\text{ch}(\lambda) = \sum_{n=0}^{+\infty} \frac{\lambda^{2n}}{(2n)!} \leq \sum_{n=0}^{+\infty} \frac{(\lambda^2/2)^n}{n!} = \exp(\frac{\lambda^2}{2})$.

Et $\varphi(\lambda) = \ln(\text{ch}(\lambda)) \leq \frac{\lambda^2}{2}$, ceci pour tout $\lambda \in \mathbb{R}$.

Deuxième preuve : On pose $\psi : \lambda \mapsto \ln(\text{ch}(\lambda)) - \frac{\lambda^2}{2}$, définie sur $\mathbb{R}$ et deux fois dérivable.

Pour tout $\lambda \in \mathbb{R}$, $\psi'(\lambda) = \frac{\text{sh}(\lambda)}{\text{ch}(\lambda)} - \lambda$ et $\psi''(\lambda) = \frac{\text{ch}^2(\lambda) - \text{sh}^2(\lambda)}{\text{ch}^2(\lambda)} - 1 = -\frac{\text{sh}^2(\lambda)}{\text{ch}^2(\lambda)} \leq 0$.

Donc ψ' est décroissante sur $\mathbb{R}$, et vérifie $\psi'(0) = 0$. Donc ψ' est positive sur $\mathbb{R}^-$ et négative sur $\mathbb{R}^+$.

Donc ψ est croissante sur $\mathbb{R}^-$ et décroissante sur $\mathbb{R}^+$. Elle admet un maximum global en 0, et $\psi(0) = \ln(1) - 0 = 0$ donc

$$\psi(\lambda) \leq 0 \text{ pour tout } \lambda \in \mathbb{R} \quad \text{soit} \quad \varphi(\lambda) \leq \frac{\lambda^2}{2}.$$

2. • Soit $t \in \mathbb{R}$ et $\lambda \in \mathbb{R}_+^*$. La variable aléatoire $\exp(\lambda S_k)$ est finie, car S_k est finie (somme finie de variables aléatoires finies), donc $\exp(\lambda S_k)$ est d'espérance finie et on peut appliquer l'**inégalité de Markov** avec $e^{\lambda t} > 0$:

$$\mathbb{P}(e^{\lambda S_k} \geq e^{\lambda t}) \leq \frac{\mathbb{E}(e^{\lambda S_k})}{e^{\lambda t}}.$$

• $e^{\lambda S_k} = \exp(\lambda(U_1 + \dots + U_k)) = \prod_{i=1}^k e^{\lambda U_i}$, et les U_i sont indépendantes donc les $e^{\lambda U_i}$ sont indépendantes ($\lambda \neq 0$).

Alors

$$\mathbb{E}(e^{\lambda S_k}) = \mathbb{E}\left(\prod_{i=1}^k e^{\lambda U_i}\right) = \prod_{i=1}^k \mathbb{E}(e^{\lambda U_i}) = (\text{ch } \lambda)^k$$

car les variables $e^{\lambda U_i}$ suivent toutes la même loi que $e^{\lambda U_1}$.

- Enfin, les événements $(e^{\lambda S_k} \geq e^{\lambda t})$ et $(S_k \geq t)$ sont égaux (car $\exp$ est strictement croissante et $\lambda > 0$). Donc

$$\mathbb{P}(S_k \geq t) = \mathbb{P}(e^{\lambda S_k} \geq e^{\lambda t}) \leq \frac{\text{ch}^k(\lambda)}{e^{\lambda t}} = \frac{(e^{\varphi(\lambda)})^k}{e^{\lambda t}} = \exp(k\varphi(\lambda) - \lambda t).$$

- En utilisant l'inégalité de 1. dans l'inégalité de 2. ($k > 0$ et $\exp$ strictement croissante), on a

$$\forall t \in \mathbb{R}, \forall \lambda > 0, \mathbb{P}(S_k \geq t) \leq \exp(k\varphi(\lambda) - \lambda t) \leq \exp(k\frac{\lambda^2}{2} - \lambda t).$$

- Prenons maintenant $t > 0$. L'inégalité précédente est vraie pour tout $\lambda > 0$, donc en choisissant $\lambda_0 = \frac{t}{k}$ ($t > 0$) on obtient $k\frac{\lambda_0^2}{2} - \lambda_0 t = k\frac{t^2}{2k^2} - \frac{t^2}{k} = -\frac{t^2}{2k}$ donc

$$\mathbb{P}(S_k \geq t) \leq \exp(k\frac{\lambda_0^2}{2} - \lambda_0 t) = \exp(-\frac{t^2}{2k}).$$

Cette majoration est optimale, puisque $\lambda_0 = \frac{t}{k}$ est la valeur de λ minimisant la fonction $\lambda \mapsto k\frac{\lambda^2}{2} - \lambda t$ donc minimisant $\lambda \mapsto \exp(k\frac{\lambda^2}{2} - \lambda t)$.

- Comme C suit une loi uniforme sur $\mathcal{M}_n(\{-1, 1\})$, on a pour tout $A \in \mathcal{M}_n(\{-1, 1\})$ fixée :

$$\mathbb{P}(C = A) = \mathbb{P}\left(\bigcap_{1 \leq i, j \leq n} C_{i,j} = a_{i,j}\right) = \frac{1}{\text{Card}(\mathcal{M}_n(\{-1, 1\}))} = \frac{1}{2^{n^2}}.$$

- Soit $(i, j) \in \llbracket 1, n \rrbracket^2$, il y a 2^{n^2-1} matrices de $\mathcal{M}_n(\{-1, 1\})$ telles que $C_{i,j} = 1$ donc

$$\mathbb{P}(C_{i,j} = 1) = \frac{\text{Card}(\{A \in \mathcal{M}_n(\{-1, 1\}) \mid a_{i,j} = 1\})}{2^{n^2}} = \frac{2^{n^2-1}}{2^{n^2}} \quad \text{donc} \quad \mathbb{P}(C_{i,j} = 1) = \frac{1}{2}.$$

Donc $C_{i,j} \sim \mathcal{U}_{\{-1, 1\}}$, ceci pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$.

- Alors pour tout $A = (a_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\{-1, 1\})$,

$$\prod_{1 \leq i, j \leq n} \mathbb{P}(C_{i,j} = a_{i,j}) = \prod_{1 \leq i, j \leq n} \frac{1}{2} = \frac{1}{2^{n^2}} = \mathbb{P}\left(\bigcap_{1 \leq i, j \leq n} C_{i,j} = a_{i,j}\right).$$

Et : pour $m \in \llbracket 1, n^2 \rrbracket$, pour $(i_1, j_1), (i_2, j_2), \dots, (i_m, j_m)$ appartenant à $\llbracket 1, n \rrbracket^2$, pour $(\varepsilon_1, \dots, \varepsilon_m) \in \{-1, 1\}^m$

$$\begin{aligned} \mathbb{P}(C_{i_1, j_1} = \varepsilon_1 \cap C_{i_2, j_2} = \varepsilon_2 \cap \dots \cap C_{i_m, j_m} = \varepsilon_m) &= \frac{\text{Card}(\{A \in \mathcal{M}_n(\{-1, 1\}) \mid a_{i_1, j_1} = \varepsilon_1, \dots, a_{i_m, j_m} = \varepsilon_m\})}{2^{n^2}} \\ &= \frac{2^{n^2-m}}{2^{n^2}} = \frac{1}{2^m} \\ &= \prod_{\ell=1}^m \mathbb{P}(C_{i_\ell, j_\ell} = \varepsilon_\ell) \end{aligned}$$

Cela prouve que les variables $(C_{i,j})_{1 \leq i, j \leq n}$ sont mutuellement indépendantes.

- Enfin, si $X = (x_1, \dots, x_n) \in \{-1, 1\}^n$ et $Y = (y_1, \dots, y_n) \in \{-1, 1\}^n$ sont fixés, **l'indépendance mutuelle des $C_{i,j}$ entraîne l'indépendance mutuelle des $x_i y_j C_{i,j}$.**

Si $x_i y_j = 1$ alors $\mathbb{P}(x_i y_j C_{i,j} = 1) = \mathbb{P}(C_{i,j} = 1) = \frac{1}{2}$; et si $x_i y_j = -1$ alors $\mathbb{P}(x_i y_j C_{i,j} = 1) = \mathbb{P}(C_{i,j} = -1) = \frac{1}{2}$.
Donc **$x_i y_j C_{i,j} \sim \mathcal{U}_{\{-1, 1\}}$.**

- Pour $t = 0$, l'inégalité est évidente : $\mathbb{P}(M(C) \geq 0) \leq 1 \leq 2^{2n} = \exp(-(0 - 2 \ln 2)n)$.
• Prenons désormais $t > 0$.

$$M(C) = \max S(C) = \max\{X^\top C Y, (X, Y) \in (\{-1, 1\}^n)^2\} = \max\left\{\sum_{1 \leq i, j \leq n} x_i y_j C_{i,j}, (X, Y) \in (\{-1, 1\}^n)^2\right\}.$$

$M(C) < tn^{3/2}$ si et seulement si pour tout $(X, Y) \in (\{-1, 1\}^n)^2$, $\sum_{1 \leq i, j \leq n} x_i y_j C_{i,j} < tn^{3/2}$:

$$(M(C) < tn^{3/2}) = \bigcap_{(X,Y) \in (\{-1,1\}^n)^2} \left(\sum_{1 \leq i,j \leq n} x_i y_j C_{i,j} < tn^{3/2} \right)$$

et en passant au complémentaire : $(M(C) \geq tn^{3/2}) = \bigcup_{(X,Y) \in (\{-1,1\}^n)^2} \left(\sum_{1 \leq i,j \leq n} x_i y_j C_{i,j} \geq tn^{3/2} \right)$.

- Par sous-additivité, $\mathbb{P}(M(C) \geq tn^{3/2}) \leq \sum_{(X,Y) \in (\{-1,1\}^n)^2} \mathbb{P} \left(\sum_{1 \leq i,j \leq n} x_i y_j C_{i,j} \geq tn^{3/2} \right)$.

Pour $(X,Y) \in (\{-1,1\}^n)^2$ fixé, en appliquant l'inégalité de Hoeffding (3.) aux variables $(x_i y_j C_{i,j})_{1 \leq i,j \leq n}$ i.i.d suivant $\mathcal{U}_{\{-1,1\}}$ (donc $k = n^2$) et avec $tn^{3/2} > 0$:

$$\mathbb{P} \left(\sum_{1 \leq i,j \leq n} x_i y_j C_{i,j} \geq tn^{3/2} \right) \leq \exp \left(-\frac{t^2 n^3}{2n^2} \right) = \exp \left(-\frac{t^2 n}{2} \right).$$

En sommant pour tous les couples $(X,Y) \in (\{-1,1\}^n)^2$:

$$\mathbb{P}(M(C) \geq tn^{3/2}) \leq \sum_{(X,Y) \in (\{-1,1\}^n)^2} \mathbb{P} \left(\sum_{1 \leq i,j \leq n} x_i y_j C_{i,j} \geq tn^{3/2} \right) \leq 2^{2n} \exp \left(-\frac{t^2 n}{2} \right)$$

car il y a $(2^n)^2 = 2^{2n}$ couples $(X,Y) \in (\{-1,1\}^n)^2$.

On a donc : $\mathbb{P}(M(C) \geq tn^{3/2}) \leq 2^{2n} \exp \left(-\frac{t^2 n}{2} \right) = \exp \left(-\frac{t^2 n}{2} + 2n \ln(2) \right) = \exp \left(-\left(\frac{t^2}{2} - 2 \ln 2\right)n \right)$.

6. • Soit $\varepsilon > 0$, prenons $t = 2\sqrt{\ln 2} + \varepsilon > 0$, alors $\mathbb{P}(M(C) \geq tn^{3/2}) \leq \exp \left(-\left(\frac{t^2}{2} - 2 \ln 2\right)n \right)$.

Or $t^2 = (2\sqrt{\ln 2} + \varepsilon)^2 > 4 \ln 2$ donc $\frac{t^2}{2} - 2 \ln 2 > 0$ et finalement $\exp \left(-\left(\frac{t^2}{2} - 2 \ln 2\right)n \right) < 1$.

Donc $\mathbb{P}(M(C) > tn^{3/2}) \leq \mathbb{P}(M(C) \geq tn^{3/2}) < 1$ et en passant au complémentaire :

$$\mathbb{P}(M(C) \leq tn^{3/2}) > 0.$$

- En particulier, l'événement $(M(C) \leq tn^{3/2})$ n'est pas impossible (donc $\neq \emptyset$). Donc il existe $\omega \in \Omega$ tel que $M(C(\omega)) \leq tn^{3/2}$ et ainsi

$$\exists C \in \mathcal{M}_n(\{-1,1\}), \quad M(C) \leq tn^{3/2} = (2\sqrt{\ln 2} + \varepsilon)n^{3/2}.$$

- Alors $\underline{M}(n) = \min\{M(A), A \in \mathcal{M}_n(\{-1,1\})\} \leq (2\sqrt{\ln 2} + \varepsilon)n^{3/2}$.

Mais cette inégalité est vérifiée pour tout $\varepsilon > 0$, et $\underline{M}(n)$ ne dépend pas de ε donc (en faisant tendre ε vers 0) :

$$\underline{M}(n) \leq 2\sqrt{\ln 2} n^{3/2}.$$

Partie III

1. • Soit $X \in \{-1,1\}^n$, alors $X^\top AY = \sum_{i=1}^n \left(x_i \sum_{j=1}^n a_{i,j} y_j \right)$.

Or pour tout $i \in \llbracket 1, n \rrbracket$, $\left(x_i \sum_{j=1}^n a_{i,j} y_j \right) \leq \left| x_i \sum_{j=1}^n a_{i,j} y_j \right| = \left| \sum_{j=1}^n a_{i,j} y_j \right|$ car $|x_i| = 1$.

En additionnant les inégalités : $X^\top AY \leq \sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} y_j \right|$.

Ceci pour tout $X \in \{-1,1\}^n$, et le majorant ne dépend pas de X , donc

$$g_A(Y) = \max\{X^\top AY, X \in \{-1,1\}^n\} \leq \sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} y_j \right|.$$

- Pour tout $i \in \llbracket 1, n \rrbracket$, notons $S_i = \sum_{j=1}^n a_{i,j} y_j$ et posons $\alpha_i = \begin{cases} 1 & \text{si } S_i \geq 0 \\ -1 & \text{si } S_i < 0 \end{cases}$

Alors $\alpha_i S_i = |S_i|$ pour tout $i \in \llbracket 1, n \rrbracket$ donc en posant $X_0 = (\alpha_i)_{1 \leq i \leq n} \in \{-1, 1\}^n$ on a

$$X_0^\top AY = \sum_{i=1}^n (\alpha_i S_i) = \sum_{i=1}^n |S_i| = \sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} y_j \right|.$$

Donc le majorant $\sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} y_j \right|$ de l'ensemble $\{X^\top AY, X \in \{-1, 1\}^n\}$ obtenu dans le premier point est une valeur atteinte par (au moins) $X_0^\top AY$ qui est un élément de l'ensemble. C'est donc le maximum de l'ensemble :

$$g_A(Y) = \sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} y_j \right|.$$

2. • $Z \sim \mathcal{U}_{\{-1, 1\}^n}$ donc pour tout $(z_1, \dots, z_n) \in \{-1, 1\}^n$, $\mathbb{P}(Z = (z_1, \dots, z_n)) = \frac{1}{2^n}$ (car $\text{Card}(\{-1, 1\}^n) = 2^n$).
• Soit $i \in \llbracket 1, n \rrbracket$. Par formule de transfert :

$$\mathbb{E} \left[\left| \sum_{j=1}^n a_{i,j} Z_j \right| \right] = \sum_{(z_1, \dots, z_n) \in \{-1, 1\}^n} \left(\left| \sum_{j=1}^n a_{i,j} z_j \right| \mathbb{P}(Z = (z_1, \dots, z_n)) \right) = \frac{1}{2^n} \sum_{(z_1, \dots, z_n) \in \{-1, 1\}^n} \left| \sum_{j=1}^n a_{i,j} z_j \right|.$$

- Soit $(z_1, \dots, z_n) \in \{-1, 1\}^n$ fixé, alors $\sum_{j=1}^n a_{i,j} z_j = k - (n - k)$ où k est le nombre de termes valant 1 dans la somme (donc $n - k$ est le nombre de termes valant -1). Comme $a_{i,1}, \dots, a_{i,n} \in \{-1, 1\}$ sont fixés, $a_{i,j} z_j = 1 \Leftrightarrow z_j = a_{i,j}$ donc

$$\sum_{j=1}^n a_{i,j} z_j = k - (n - k) = 2k - n \quad \text{où } k = \text{Card}\{j \in \llbracket 1, n \rrbracket, z_j = a_{i,j}\}.$$

- Dans le point précédent, k peut prendre les valeurs 0 à n donc on peut écrire (sommation par paquets, même si c'est une somme finie). Notons $E_k = \{(z_1, \dots, z_n) \in \{-1, 1\}^n \mid \text{Card}\{j, z_j = a_{i,j}\} = k\}$:

$$\mathbb{E} \left[\left| \sum_{j=1}^n a_{i,j} Z_j \right| \right] = \frac{1}{2^n} \sum_{k=0}^n \left(\sum_{(z_1, \dots, z_n) \in E_k} |2k - n| \right).$$

Comme $|2k - n|$ ne dépend pas de $(z_1, \dots, z_n) \in E_k$, on peut écrire : $\sum_{(z_1, \dots, z_n) \in E_k} |2k - n| = |2k - n| \text{Card}(E_k)$.

Or un élément de E_k est déterminé de manière unique par la donnée de k indices $j_1, \dots, j_k$ parmi les n entiers de $\llbracket 1, n \rrbracket$ tels que $a_{i,j_1} = z_{j_1}, \dots, a_{i,j_k} = z_{j_k}$, donc :

$$\text{Card}(E_k) = \binom{n}{k} \text{ pour tout } k \in \llbracket 0, n \rrbracket \quad \text{et finalement} \quad \mathbb{E} \left[\left| \sum_{j=1}^n a_{i,j} Z_j \right| \right] = \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} |2k - n|.$$

- Enfin, $\mathbb{E}[g_A(Z)] \stackrel{\text{III.1}}{=} \mathbb{E} \left[\sum_{i=1}^n \left| \sum_{j=1}^n a_{i,j} Z_j \right| \right] = \sum_{i=1}^n \mathbb{E} \left[\left| \sum_{j=1}^n a_{i,j} Z_j \right| \right]$ par linéarité de l'espérance.

Or les n termes $\mathbb{E} \left[\left| \sum_{j=1}^n a_{i,j} Z_j \right| \right]$ ont une valeur qui ne dépend pas de i (ils sont tous égaux)

$$\mathbb{E}[g_A(Z)] = n \mathbb{E} \left[\left| \sum_{j=1}^n a_{1,j} Z_j \right| \right] = \frac{n}{2^n} \sum_{k=0}^n \binom{n}{k} |n - 2k|.$$

3. (a) • Si $n = 1$, on prend seulement $m = 0$, donc $\sum_{k=0}^0 (1 - 2k) \binom{1}{k} = 1 \binom{1}{0}$, la propriété est vérifiée.

Dans la suite, on suppose $n \geq 2$.

- Pour $m = 0$, la somme ne contient que le terme $k = 0$, elle vaut $n \binom{n}{0} = n = n \binom{n-1}{0}$.
- Soit $m \in \llbracket 1, n - 1 \rrbracket$, alors pour tout $k \in \llbracket 1, m \rrbracket$, avec la symétrie des coefficients binomiaux ($\binom{n}{k} = \binom{n}{n-k}$) et la formule du capitaine ($j \binom{n}{j} = n \binom{n-1}{j-1}$ si $j \geq 1$) :

$$(n-2k)\binom{n}{k} = (n-k)\binom{n}{n-k} - k\binom{n}{k} = n\left(\binom{n-1}{n-k-1} - \binom{n-1}{k-1}\right) = n\left(\binom{n-1}{k} - \binom{n-1}{k-1}\right).$$

$$\text{Donc } \sum_{k=0}^m \binom{n}{k}(n-2k) = \binom{n}{0}n + \sum_{k=1}^m n\left(\binom{n-1}{k} - \binom{n-1}{k-1}\right) = n + n\sum_{k=1}^m \left(\binom{n-1}{k} - \binom{n-1}{k-1}\right).$$

On reconnaît un télescopage : $\sum_{k=1}^m \left(\binom{n-1}{k} - \binom{n-1}{k-1}\right) = \binom{n-1}{m} - \binom{n-1}{0} = \binom{n-1}{m} - 1$ donc

$$\sum_{k=0}^m \binom{n}{k}(n-2k) = n + n\left(\binom{n-1}{m} - 1\right) = n\binom{n-1}{m}.$$

Penser à traiter à part les cas particuliers $n=1$ ou $m=0$ n'est pas crucial. Mais sortir le terme $k=0$ de la somme est indispensable pour appliquer la formule du capitaine aux coefficients binomiaux de la somme et pour que le télescopage s'arrange bien.

(b) • Pour $k \in \llbracket 0, n \rrbracket$, $n-2k \geq 0 \Leftrightarrow k \leq \frac{n}{2} \Leftrightarrow k \leq \lfloor \frac{n}{2} \rfloor$ donc en notant $m = \lfloor \frac{n}{2} \rfloor \leq n-1$:

$$\sum_{k=0}^n \binom{n}{k}|n-2k| = \sum_{k=0}^m \binom{n}{k}(n-2k) + \sum_{k=m+1}^n \binom{n}{k}(2k-n) = \sum_{k=0}^m \binom{n}{k}(n-2k) - \left(\sum_{k=0}^n \binom{n}{k}(n-2k) - \sum_{k=0}^m \binom{n}{k}(n-2k) \right)$$

$$\sum_{k=0}^n \binom{n}{k}(n-2k) = \sum_{k=0}^{n-1} \binom{n}{k}(n-2k) + (n-2n)\binom{n}{n} \stackrel{(a)}{=} n\binom{n-1}{n-1} - n = 0 \text{ donc}$$

$$\sum_{k=0}^n \binom{n}{k}|n-2k| = 2 \sum_{k=0}^m \binom{n}{k}(n-2k) \stackrel{(a)}{=} 2n\binom{n-1}{m}$$

• Soit $A \in \mathcal{M}_n(\{-1, 1\})$. En reportant le résultat ci-dessus dans l'expression prouvée en 2. :

$$\mathbb{E}[g_A(Z)] = \frac{n}{2^n} \sum_{k=0}^n \binom{n}{k}|n-2k| = \frac{n}{2^n} \times (2n)\binom{n-1}{m} = \frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor}.$$

4. (a) • Soit $A \in \mathcal{M}_n(\{-1, 1\})$, soit Z une variable uniforme sur $\{-1, 1\}^n$, alors

$$g_A(Z) = \max\{X^\top AZ, X \in \{-1, 1\}^n\} \leq M(A) = \max\{X^\top AY, (X, Y) \in (\{-1, 1\}^n)^2\}$$

La variable aléatoire $g_A(Z)$ est majorée par la constante $M(A)$, donc son espérance est majorée par cette même constante :

$$\mathbb{E}[g_A(Z)] = \frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor} \leq M(A).$$

• L'inégalité précédente est vraie pour tout $A \in \mathcal{M}_n(\{-1, 1\})$ et le terme de gauche ne dépend finalement pas de A (seulement de n). Donc

$$\frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor} \leq \min\{M(A), A \in \mathcal{M}_n(\{-1, 1\})\} = \underline{M}(n).$$

(b) *Appliquer la formule de Stirling avec une partie entière (car $\binom{n-1}{\lfloor \frac{n}{2} \rfloor} = \frac{(n-1)!}{(\lfloor \frac{n}{2} \rfloor)!(n-\lfloor \frac{n}{2} \rfloor)!}$) me semble risqué... je sépare donc les cas n pair et n impair.*

* Si $n = 2m$ est pair, alors $m = \frac{n}{2} = \lfloor \frac{n}{2} \rfloor \xrightarrow{n \rightarrow +\infty} +\infty$ et

$$\frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor} = \frac{4m^2}{2^{2m-1}} \frac{(2m-1)!}{m!(m-1)!} = \frac{4m^2}{2^{2m-1}} \frac{(2m)!}{2(m!)^2} \underset{m \rightarrow +\infty}{\sim} \frac{4m^2}{2^{2m}} \frac{\sqrt{4\pi m}(2m/e)^{2m}}{2\pi m(m/e)^{2m}} = \frac{4m^2}{2^{2m}} \frac{\sqrt{\pi m} 2^{2m}}{\pi m} = \frac{4m\sqrt{m}}{\sqrt{\pi}}$$

* Si $n = 2m+1$ est impair, alors $m = \frac{n-1}{2} = \lfloor \frac{n}{2} \rfloor \xrightarrow{n \rightarrow +\infty} +\infty$ et

$$\frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor} = \frac{(2m+1)^2}{2^{2m}} \frac{(2m)!}{(m!)^2} \underset{m \rightarrow +\infty}{\sim} \frac{4m^2}{2^{2m}} \frac{\sqrt{4\pi m}(2m/e)^{2m}}{2\pi m(m/e)^{2m}} = \frac{4m\sqrt{m}}{\sqrt{\pi}}$$

On obtient le même équivalent, avec $m = \lfloor \frac{n}{2} \rfloor$. Il reste à écrire cela en fonction de n (et pas en fonction de $\lfloor \frac{n}{2} \rfloor$).

On a $\frac{n}{2} - 1 < \lfloor \frac{n}{2} \rfloor \leq \frac{n}{2}$ et $\frac{n}{2} - 1 \underset{n \rightarrow +\infty}{\sim} \frac{n}{2}$ donc par encadrement : $\lfloor \frac{n}{2} \rfloor \underset{n \rightarrow +\infty}{\sim} \frac{n}{2}$. Donc

$$\frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor \frac{n}{2} \rfloor} \underset{n \rightarrow +\infty}{\sim} \frac{4(n/2)\sqrt{n/2}}{\sqrt{\pi}} = \frac{\sqrt{2}}{\sqrt{\pi}} n\sqrt{n} = \sqrt{\frac{2}{\pi}} n^{3/2}.$$

On obtient un minorant ayant (pour n grand) le même ordre de grandeur que le majorant : $n^{3/2}$. Plus précisément, $\sqrt{\frac{2}{\pi}} \simeq 0,8$ et $2\sqrt{\ln 2} \simeq 1,7...$

Partie IV

Démonstration de la formule de Stirling en passant par des intégrales et le théorème de convergence dominée. Moins élémentaire que celle vue en TD en début d'année. Cette démonstration avec des intégrales a aussi été vue dans un sujet des Mines il me semble...

1. *Tellement classique ! On remarque que le mot "récurrence" est dans la question... On peut justifier la relation entre I_{n+1} et I_n dans un premier temps, puis rédiger la récurrence pour la valeur de I_n , ou bien on se souvient et on fait tout en même temps.*

- Pour tout $n \in \mathbb{N}$, $x \mapsto x^n e^{-x}$ est continue sur $[0, +\infty[$ et $x^n e^{-x} \underset{x \rightarrow +\infty}{=} o\left(\frac{1}{x^2}\right)$ par croissance comparée, donc la fonction est intégrable en $+\infty$. Ainsi, I_n est bien définie pour tout $n \in \mathbb{N}$.
- Montrons par récurrence sur $n \in \mathbb{N}$ que $I_n = n!$

* $I_0 = \int_0^{+\infty} e^{-x} dx = 1 = 0!$, la propriété est vraie au rang 0.

* Soit $n \in \mathbb{N}$, supposons la propriété vraie au rang n .

$-x^{n+1}e^{-x} \underset{x \rightarrow +\infty}{\longrightarrow} 0$ donc on peut effectuer l'intégration par parties sur I_{n+1} :

$$I_{n+1} = [x^{n+1}(-e^{-x})]_0^{+\infty} - \int_0^{+\infty} (n+1)x^n \cdot (-e^{-x}) dx = 0 + (n+1)I_n.$$

Par hypothèse de récurrence, $I_n = n!$ donc $I_{n+1} = (n+1) \times (n!) = (n+1)!$, la propriété est vraie au rang $n+1$.

$$2. \text{ Soit } n \geq 1, \int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx \underset{t=n+\sqrt{n}x}{=} \int_0^{+\infty} \left(\frac{t}{n}\right)^n e^{n-t} \frac{1}{\sqrt{n}} dt = \frac{e^n}{n^n \sqrt{n}} I_n$$

donc on a bien : $I_n = \left(\frac{n}{e}\right)^n \sqrt{n} \int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx.$

3. (a) Soit $(t, x) \in U$ avec $x \leq 0$ (i.e. $t > 0$ et $0 \geq x > -t$), alors $0 \leq \frac{x}{t} > -1$ donc on peut utiliser le développement en série entière de $u \mapsto \ln(1+u)$:

$$\begin{aligned} f(t, x) &= t^2 \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} \left(\frac{x}{t}\right)^n - xt = t^2 \left(\frac{x}{t} - \frac{x^2}{2t^2} - \sum_{n=3}^{+\infty} \frac{(-x)^n}{nt^n} \right) - xt \\ &= \frac{-x^2}{2} - \sum_{n=3}^{+\infty} \frac{|x|^n}{nt^{n-2}} \quad \text{car } x \leq 0 \text{ donc } -x = |x| \end{aligned}$$

Or $\sum_{n=3}^{+\infty} \frac{|x|^n}{nt^{n-2}} \geq 0$ car somme d'une série (convergente) à termes positifs. Donc on a bien :

$$f(t, x) \leq -\frac{x^2}{2} \text{ si } x \leq 0.$$

- (b) • Dans cette question, on fixe $x > 0$ et on étudie la fonction partielle $t \mapsto f(t, x)$ sur $[1, +\infty[$ (sa dérivée se note donc $\frac{\partial f}{\partial t}(t, x)$).

$$\forall t \geq 1, \frac{\partial f}{\partial t}(t, x) = 2t \ln\left(1 + \frac{x}{t}\right) + t^2 \left(\frac{-x}{t^2} \times \frac{1}{1+\frac{x}{t}} \right) - x = t \left[2 \ln\left(1 + \frac{x}{t}\right) - \frac{x}{t} \times \frac{1}{1+\frac{x}{t}} - \frac{x}{t} \right] = tF\left(\frac{x}{t}\right)$$

avec $F : u \mapsto 2 \ln(1+u) - \frac{u}{1+u} - u$, que l'on étudie sur $\mathbb{R}_+^*$ car $x > 0$ et $t \geq 1$ (donc la condition $x > -t$ est automatiquement vérifiée), donc $u = xt > 0$.

$$\bullet \forall u > 0, F'(u) = \frac{2}{1+u} - \frac{1}{(1+u)^2} - 1 = \frac{-u^2}{(1+u)^2} < 0.$$

Donc F est strictement décroissante sur $\mathbb{R}_+^*$. Sa borne supérieure est sa limite en 0 : $\sup_{u>0} F(u) = 0$ donc F

est strictement négative sur $\mathbb{R}_+^*$.

Toutes les inégalités strictes sont des informations facilement accessibles ici, mais pas du tout indispensables ! On aurait pu étudier F sur $\mathbb{R}^+$ et obtenir qu'elle est négative ou nulle sur $\mathbb{R}^+$.

- Ainsi, pour $t \geq 1$, $\frac{\partial f}{\partial t}(t, x) = tF\left(\frac{x}{t}\right) \leq 0$ (avec $x > 0$ fixé) donc $t \mapsto f(t, x)$ est décroissante sur $[1, +\infty[$. On en déduit :

$$\forall t \geq 1, f(t, x) \leq f(1, x).$$

4. D'après 1. et 2. on a : $\frac{I_n}{\sqrt{n(n/e)^n}} = \frac{n!}{\sqrt{n(n/e)^n}} = \int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx = J_n$ pour tout $n \geq 1$.

De plus, $J_n = \int_{-\infty}^{+\infty} g_n(x) dx$ où $g_n : \mathbb{R} \rightarrow \mathbb{R}$ est définie par :

$$g_n(x) = \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} \mathbf{1}_{[-\sqrt{n}, +\infty[} = \begin{cases} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} & \text{si } x > -\sqrt{n} \\ 0 & \text{sinon} \end{cases}$$

Pour $x > -\sqrt{n}$, $\ln(g_n(x)) = n \ln\left(1 + \frac{x}{\sqrt{n}}\right) - x\sqrt{n} = f(\sqrt{n}, x)$ avec la notation de 3. ($t = \sqrt{n}$ avec $n \in \mathbb{N}^*$, on a bien $t > 0$ et $x > -t$ ici).

Théorème de convergence dominée, avec une fonction dépendant d'une INDICATRICE :

* CVS : Soit $x \in \mathbb{R}$, alors à partir d'un certain rang, $g_n(x) = \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}}$.

Plus précisément, cette égalité est vraie pour n tel que $x > -\sqrt{n}$ donc pour tout $n \geq 1$ si $x \geq 0$, et seulement pour $n > x^2$ si $x < 0$.

Donc à partir d'un certain rang,

$$\ln(g_n(x)) = n \ln\left(1 + \frac{x}{\sqrt{n}}\right) - x\sqrt{n} \underset{n \rightarrow +\infty}{=} n \left(\frac{x}{\sqrt{n}} - \frac{x^2}{2n} + o\left(\frac{1}{n}\right)\right) - x\sqrt{n} \underset{n \rightarrow +\infty}{=} -\frac{x^2}{2} + o(1)$$

Donc la suite de fonction (g_n) converge simplement sur $\mathbb{R}$, vers la fonction $x \mapsto e^{-x^2/2}$.

* HD : Soit $x \in \mathbb{R}$, soit $n \in \mathbb{N}^*$. D'après 3. on a :

$$(i) |g_n(x)| = g_n(x) \underset{\text{si } x > -\sqrt{n}}{=} \exp(f(\sqrt{n}, x)) \leq e^{-x^2/2} \quad \text{si } -\sqrt{n} < x \leq 0;$$

$$(ii) |g_n(x)| = 0 \leq e^{-x^2/2} \quad \text{si } x \leq -\sqrt{n};$$

$$(iii) |g_n(x)| = \exp(f(\sqrt{n}, x)) \leq \exp(f(1, x)) = (1+x)e^{-x} \quad \text{si } x > 0 \text{ (on a toujours } x > -\sqrt{n} \text{ dans ce cas).}$$

Donc on a l'hypothèse de domination : $\forall x \in \mathbb{R}, \forall n \in \mathbb{N}^*, |g_n(x)| \leq g(x) = \begin{cases} e^{-x^2/2} & \text{si } x \leq 0 \\ (1+x)e^{-x} & \text{si } x > 0 \end{cases}$

La fonction g est continue par morceaux sur $\mathbb{R}$, et indépendante du paramètre n (en fait elle est bien continue en 0 car $\lim_{x \rightarrow 0^+} g(x) = 1 = g(0)$ mais ce n'est pas important !)

De plus, $e^{-x^2/2} \underset{x \rightarrow -\infty}{=} o\left(\frac{1}{x^2}\right)$, intégrable en $-\infty$; et $(1+x)e^{-x} \underset{x \rightarrow +\infty}{\sim} xe^{-x} \underset{x \rightarrow +\infty}{=} o\left(\frac{1}{x^2}\right)$, intégrable en $+\infty$.

Donc g est intégrable sur $\mathbb{R}$.

C/c : Toutes les hypothèses du théorème étant vérifiées, on obtient :

$$\lim_{n \rightarrow +\infty} J_n = \int_{-\infty}^{+\infty} \left(\lim_{n \rightarrow +\infty} g_n(x) \right) dx = \int_{-\infty}^{+\infty} e^{-x^2/2} dx = \sqrt{2\pi}$$

(intégrale de Gauss, valeur donnée dans l'énoncé).

Donc $\frac{n!}{\sqrt{n(n/e)^n}} = J_n \underset{n \rightarrow +\infty}{\longrightarrow} \sqrt{2\pi}$, soit $n! \underset{n \rightarrow +\infty}{\sim} \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

Partie V

1. $A \in \mathcal{M}_n(\{-1, 1\})$ et $Y \in \{-1, 1\}^n$ sont fixés.

• Montrons par récurrence que, pour tout $p \in \mathbb{N}^*$, si $(x_1, \dots, x_p) \in \mathbb{Z}^p$ est tel que pour tout $i \in \llbracket 1, p \rrbracket$, $|x_i| \leq n$ alors il existe des $\varepsilon_i \in \{-1, 1\}$ tel que $|\varepsilon_1 x_1 + \dots + \varepsilon_p x_p| \leq n$.

(i) Évident pour $p = 1$. Vérifions le pour $p = 2$ (utile pour l'hérédité) : soit $(x_1, x_2) \in \mathbb{Z}^2$ tel que $|x_1| \leq n$ et $|x_2| \leq n$, i.e. $(x_1, x_2) \in [-n, n]^2$.

Si $(x_1, x_2) \in [0, n]^2$, alors $-n \leq x_1 - x_2 \leq n$, i.e. $|x_1 - x_2| \leq n$. De même si $(x_1, x_2) \in [-n, 0]^2$.

Si x_1 et x_2 ne sont pas de même signe (l'un appartenant à $[0, n]$ et l'autre à $[-n, 0]$), alors en remplaçant x_2 par $-x_2$ on retombe sur les premiers cas donc on a $|x_1 - (-x_2)| = |x_1 + x_2| \leq n$.

Dans tous les cas, on a trouvé $\varepsilon \in \{-1, 1\}$ tel que $|x_1 + \varepsilon x_2| \leq n$, la propriété est vérifiée au rang 2.

(ii) Supposons la propriété vraie au rang p (un certain $p \in \mathbb{N}^*$ étant fixé). Soit $(x_1, \dots, x_p, x_{p+1}) \in \mathbb{Z}^{p+1}$ tel que $|x_i| \leq n$ pour tout i .

Par hypothèse de récurrence, il existe $(\varepsilon_1, \dots, \varepsilon_p) \in \{-1, 1\}^p$ tel que $|\varepsilon_1 x_1 + \dots + \varepsilon_p x_p| \leq n$ et d'après la propriété au rang 2, comme on a aussi $|x_{p+1}| \leq n$, on peut trouver $\varepsilon_{p+1} \in \{-1, 1\}$ tel que

$$|(\varepsilon_1 x_1 + \dots + \varepsilon_p x_p) + \varepsilon_{p+1} x_{p+1}| \leq n$$

- Pour tout $i \in \llbracket 1, n \rrbracket$, $|(AY)_i| = \left| \sum_{j=1}^n a_{i,j} y_j \right| \leq \sum_{j=1}^n |a_{i,j} y_j| \leq n$ (somme de n termes inférieurs à 1).

On dispose donc des ε_i tel que $|\varepsilon_1 (AY)_1 + \dots + \varepsilon_p (AY)_p| \leq n$.

Posons $X_0 = \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_p \end{pmatrix}$, on a alors $|X_0^\top AY| \leq n$.

On a donc montré que $\min \{|X^\top AY| \mid X \in \{-1, 1\}^n\} \leq n$ (puisque l'un des éléments de cet ensemble est inférieur ou égal à n).

- Comme $S(A)$ est symétrique, $\min(S(A) \cap \mathbb{N}) = \min(|s| \mid s \in S(A))$. D'où

$$m(A) = \min \left\{ \underbrace{\min \{|XAY| \mid X \in \{-1, 1\}^n\}}_{\leq n} \mid Y \in \{-1, 1\}^n \right\} \leq n.$$

2. Soit $\varepsilon > 0$. Posons $t = \sqrt{2n \ln(2n)} + \varepsilon$ de sorte que $2n \exp\left(-\frac{t^2}{2n}\right) < 1$.

Introduisons une variable aléatoire uniforme Z comme à la question III.2).

Utilisons l'inégalité de Hoeffding établie à la question II.3), on a à $i \in \llbracket 1, n \rrbracket$ fixé,

$$\mathbb{P} \left(\sum_{j=1}^n a_{i,j} Z_j \geq t \right) \leq \exp\left(-\frac{t^2}{2n}\right) \quad \text{en prenant } S_n = \sum_{j=1}^n \underbrace{a_{i,j} Z_j}_{=U_j \text{ de la partie II}}.$$

De même avec $-S_n$, $\mathbb{P} \left(-\sum_{j=1}^n a_{i,j} Z_j \geq t \right) \leq \exp\left(-\frac{t^2}{2n}\right)$, donc, finalement,

$$\mathbb{P} \left(\left| \sum_{j=1}^n a_{i,j} Z_j \right| \geq t \right) \leq 2 \exp\left(-\frac{t^2}{2n}\right).$$

Avec la sous-additivité :

$$\mathbb{P} \left(\exists i \in \llbracket 1, n \rrbracket, \left| \sum_{j=1}^n a_{i,j} Z_j \right| \geq t \right) = \mathbb{P} \left(\bigcup_{i=1}^n \left(\left| \sum_{j=1}^n a_{i,j} Z_j \right| \geq t \right) \right) \leq \sum_{i=1}^n \mathbb{P} \left(\left| \sum_{j=1}^n a_{i,j} Z_j \right| \geq t \right) \leq 2n \exp\left(-\frac{t^2}{2n}\right)$$

Comme $2n \exp\left(-\frac{t^2}{2n}\right) < 1$, en passant au complémentaire on a

$$\mathbb{P} \left(\bigcap_{i=1}^n \left(\left| \sum_{j=1}^n a_{i,j} Z_j \right| < t \right) \right) > 0 \quad \text{donc} \quad \bigcap_{i=1}^n \left(\left| \sum_{j=1}^n a_{i,j} Z_j \right| < t \right) \neq \emptyset.$$

Il existe $\omega \in \Omega$ tel que, $\forall i \in \llbracket 1, n \rrbracket$, $\left| \sum_{j=1}^n a_{i,j} (Z(\omega))_j \right| < t$.

Ainsi, pour $Y = Z(\omega) \in \{-1, 1\}^n$, on a $\left| \sum_{j=1}^n a_{i,j} Y_j \right| < t$.

Ensuite, en reprenant l'idée de V.1, on montre qu'il existe $X \in \{-1, 1\}^n$ tel que $|X^\top AY| < t$ (on remplace le majorant n par t).

Donc $m(A) < t$, cette inégalité étant vraie pour tout $\varepsilon > 0$, on obtient en faisant tendre ε vers 0,

$$m(A) \leq \sqrt{2n \ln(2n)}.$$