

Corrigé : X-ENS-ESPCI PC 2018

Thomas CHEN

I Partie I

I.1. Pour choisir M dans $\mathcal{M}_n(\{-1, 1\})$, il faut choisir $[M]_{i,j}$ pour tout $i, j \in \llbracket 1, n \rrbracket$. Comme il n'y a que deux choix possible pour chaque coefficient de M , on a $\boxed{2^{n^2} \text{ matrices dans } \mathcal{M}_n(\{-1, 1\})}$.

Cependant, $\mathcal{M}_n(\{-1, 1\})$ n'est pas un espace vectoriel puisqu'il ne contient pas la matrice nulle.

I.2. Soit $X = (x_i)_{1 \leq i \leq n}, Y = (y_j)_{1 \leq j \leq n} \in \{-1, 1\}^n, A = (a_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\{-1, 1\})$.

- Alors

$$X^T(AY) = \sum_{i=1}^n x_i [AY]_i = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} x_i y_j.$$

Or,

$$\forall i, j \in \llbracket 1, n \rrbracket, -1 \leq a_{i,j} x_i y_j \leq 1$$

donc

$$-n^2 = \sum_{i=1}^n \sum_{j=1}^n -1 \leq \sum_{i=1}^n \sum_{j=1}^n a_{i,j} x_i y_j \leq \sum_{i=1}^n \sum_{j=1}^n 1 = n^2.$$

Ainsi, $X^T AY \in \llbracket -n^2, n^2 \rrbracket$. Ainsi,

$$\boxed{S(A) \subset \llbracket -n^2, n^2 \rrbracket}.$$

- Comme $a_{i,j} x_i y_j \in \{-1, 1\}$ pour tout $i, j \in \llbracket 1, n \rrbracket$, $X^T AY$ a la même parité que n^2 en tant que somme de n^2 éléments impairs.

Puisque n^2 et $n^2 - 1$ n'ont pas la même parité, $X^T AY$ ne peut évaluer $n^2 - 1$, et ce, pour tout $X, Y \in \{-1, 1\}^n$. On en déduit que $n^2 - 1 \notin S(A)$ donc

$$\boxed{S(A) \subsetneq \llbracket -n^2, n^2 \rrbracket}.$$

- Soit $k \in S(A)$. Alors il existe $X, Y \in \{-1, 1\}^n$ tel que $X^T AY = k$. Comme $-X \in \{-1, 1\}^n$ et $(-X)^T AY = -k$, on a bien $-k \in S(A)$. $\boxed{S(A) \text{ est bien symétrique.}}$

I.3. Soit $X = (x_i)_{1 \leq i \leq n}, Y = (y_j)_{1 \leq j \leq n} \in \{-1, 1\}^n$. Notons $C = \text{diag}(c_1, \dots, c_n), D = \text{diag}(d_1, \dots, d_n)$.

Multiplier par des matrices diagonales, c'est censé être rapide. Je rappelle ici le résultat. Soit $M \in \mathcal{M}_n(\mathbb{K})$. On l'écrit en colonnes et en lignes :

$$M = (C_1 \mid \cdots \mid C_n) = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix}.$$

Notons $D = \text{diag}(d_1, \dots, d_n)$, $\Delta = \text{diag}(\delta_1, \dots, \delta_n)$. Alors

$$DM = \begin{pmatrix} c_1 L_1 \\ \vdots \\ c_n L_n \end{pmatrix}; \quad M\Delta = (\delta_1 C_1 \mid \cdots \mid \delta_n C_n).$$

Quand on multiplie une matrice par une matrice diagonale à **gauche**, on agit sur les **lignes**. Si c'est à **droite**, on agit sur les **colonnes**.

Alors $X^T C = (C^T X)^T = (CX)^T$ est aussi dans $\{-1, 1\}$ puisque

$$CX = \begin{pmatrix} c_1 x_1 \\ \vdots \\ c_n x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\{-1, 1\})$$

et de même pour DY . Alors

$$X^T B Y = X^T C A D Y = (CX)^T A D Y \in S(A)$$

Ceci étant vrai pour tout $X, Y \in \{-1, 1\}^n$, on en déduit que $S(B) \subset S(A)$. Comme $C^2 = I_n$ et $D^2 = I_n$, on a $A = CBD$ donc de même, $S(B) \subset S(A)$. Ainsi,

$$S(A) = S(B).$$

I.4. $S(I) = \{X^T I Y : X, Y \in \{-1, 1\}^2\} = \{x_1 y_1 + x_2 y_1 + x_1 y_2 + x_2 y_2 : x_1, x_2, y_1, y_2 \in \{-1, 1\}\}$. La question 2 assure que

$$S(I) \subset \llbracket -4, -2, 0, 2, 4 \rrbracket.$$

$4 \in S(I)$ puisque $\begin{pmatrix} 1 \\ 1 \end{pmatrix}^T I \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 4$. Par la question 2, $-4 \in I$. On a aussi $0 \in S(I)$ puisque

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}^T I \begin{pmatrix} -1 \\ 1 \end{pmatrix} = 0$$

Pour que 2 soit dans $S(A)$, il faut et suffit de trouver $x_1, x_2, y_1, y_2 \in \{-1, 1\}$ tel que $x_1 y_1 + x_2 y_1 + x_1 y_2 + x_2 y_2$ ce qui revient à dire que 3 des 4 termes sont positifs (donc égaux à 1) et le dernier négatif (donc égal à -1 pour compenser), disons les 3 premiers. Alors l'égalité

$$x_1 y_1 = 1$$

entraîne $x_1 = y_1$. De même, $x_2 y_1 = 1$ donc $x_2 = y_1$ et enfin, $x_1 = y_2$. On en déduit que $x_2 = y_2$ donc $x_2 y_2 = 1$. En contraposant, on a bien que $2 \notin S(A)$ donc $-2 \notin S(A)$ par la question 2.

Finalement, on a

$$\boxed{S(I) = \{-4, 0, 4\}}.$$

On a

$$J = I + \begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix}$$

donc $\forall X = (x_1, x_2), Y = (y_1, y_2) \in \{-1, 1\}^n, X^T J Y = X^T I Y - 2x_2 y_2$. On en déduit que

$$S(J) \subset \{r + 2 : r \in S(I)\} \cup \{r - 2 : r \in S(I)\} = \{-6, -2, 2, 6\}.$$

Or, $S(J) \subset \{-4, -2, 0, 2, 4\}$ donc $S(J) \subset \{-2, 2\}$. En prenant $X = Y = (1, 1)$, on a $X^T J X = X^T I X - 2 = 4 - 2 = 2$ donc $\{-2, 2\} \in S(J)$. On a bien

$$\boxed{S(J) = \{-2, 2\}}.$$

I.5. Il est classique de savoir montrer que A est de rang 1 si, et seulement si, A s'écrit XY^T où $X, Y \in \mathcal{M}_{n,1}(\mathbb{K}) \setminus \{0\}$. On va donc montrer (a) \iff (b) et (b) \iff (c).

(b) \implies (c) Soit $X, Y \in \{-1, 1\}^n$ et $A = XY^T$. Alors en notant $(y_1 \cdots y_n) = Y^T$, on a

$$A = (y_1 X \mid \cdots \mid y_n X)$$

donc les colonnes de A sont engendrées par $X \neq 0$: A est de rang 1.

(c) \implies (b) Soit A de rang 1. Notons $A = (C_1 \mid \cdots \mid C_n)$. Comme A est de rang 1, A n'est pas nulle : soit donc X une colonne non nulle de A . Comme A est à coefficients dans $\{-1, 1\}$, X l'est aussi.

Par ailleurs, $\text{Vect}(C_1, \dots, C_n) \subset \text{Vect}(X)$ et $\dim(\text{Vect}(C_1, \dots, C_n)) = \text{rg}(A) = 1$ donc

$$\text{Vect}(C_1, \dots, C_n) = \text{Vect}(X)$$

i.e. il existe $y_1, \dots, y_n \in \mathbb{R}$ tels que $\forall i \in \llbracket 1, n \rrbracket, C_i = y_i X$. On a donc $A = XY^T$ où $Y^T = (y_1 \cdots y_n)$. Or, pour tout $i, j \in \llbracket 1, n \rrbracket$, le coefficient en (i, j) de A est $y_i x_j \in \{-1, 1\}$. Comme $x_j \in \{-1, 1\}$, on a alors $y_i \in \{-1, 1\}$ et ce, pour tout $i \in \llbracket 1, n \rrbracket$: on en déduit que $Y \in \{-1, 1\}^n$.

Il existe donc $X, Y \in \{-1, 1\}^n$ tels que $A = XY^T$.

(b) \implies (a) Soit $X = (x_i)_{1 \leq i \leq n}, Y = (y_j)_{1 \leq j \leq n} \in \{-1, 1\}^n$ et $A = XY^T$. Alors

$$X^T A Y = (X^T X)(Y^T Y) = \sum_{k=1}^n x_k^2 \sum_{j=1}^n y_j^2 = n^2$$

donc $n^2 \in S(A)$.

(a) \implies (b) Si $n^2 \in S(A)$, alors il existe $X = (x_i)_{1 \leq i \leq n}, Y = (y_j)_{1 \leq j \leq n} \in \{-1, 1\}^n$ tels que $X^T A Y = n^2$. Notons $(a_{i,j})$ le coefficient en (i, j) de A . On a alors

$$n^2 = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} x_i y_j \leq \sum_{i=1}^n \sum_{j=1}^n 1 = n^2$$

donc

$$\forall i, j \in \llbracket 1, n \rrbracket, a_{i,j} x_i y_j = 1$$

i.e.

$$\forall i, j \in \llbracket 1, n \rrbracket, a_{i,j} (x_i y_j)^2 = a_{i,j} = x_i y_j$$

donc $A = XY^T$ par l'égalité coefficient par coefficient.

I.6. Pour obtenir une matrice qui vérifie $n^2 \in S(A)$, il faut et suffit que A s'écrive XY^T . Il faut donc choisir la première colonne (n coefficients à choisir) puis choisir par quoi on multiplie cette colonne pour obtenir les $n - 1$ autres (donc $n - 1$ coefficients à choisir). Cela fait au total $2n - 1$ coefficients à choisir dans $\{-1, 1\}$ donc 2^{2n-1} matrices A vérifiant $n^2 \in S(A)$.

Ainsi, la proportion cherchée est

$$\boxed{\frac{\text{nombre de matrices } A \text{ vérifiant } n^2 \in S(A)}{\text{Card}(\mathcal{M}_n(\{-1, 1\}))} = \frac{2^{2n-1}}{2^{n^2}} = \frac{1}{2^{(n-1)^2}}.}$$

II Partie II

Remarque culturelle : une variable aléatoire X à valeurs dans $\{-1, 1\}$ est dite loi de Rademacher de paramètre $\mathbb{P}(X = 1)$. Ici, les $(U_i)_{1 \leq i \leq k}$ suivent une loi de Rademacher de paramètre $\frac{1}{2}$.

II.1. Soit $\lambda \in \mathbb{R}$. Soit $f : x \in \mathbb{R} \mapsto e^{\lambda x} \in \mathbb{R}$. Alors par le théorème de transfert,

$$\mathbb{E}[f(U_1)] = \sum_{\omega \in U_1(\omega)} f(\omega) \mathbb{P}(U_1 = \omega) = \frac{f(1)}{2} + \frac{f(-1)}{2} = \cosh(\lambda).$$

Or,

$$\forall t \in \mathbb{R}, \forall n \in \mathbb{N}, \frac{t^{2n}}{(2n)!} \leq \frac{t^{2n}}{2^n n!}$$

donc on a l'inégalité (très classique¹)

$$\cosh(t) = \sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n)!} \leq \sum_{n=0}^{+\infty} \frac{t^{2n}}{2^n n!} = e^{t^2/2}.$$

On en déduit que

$$\forall \lambda \in \mathbb{R}, \exp(\varphi(\lambda)) = \cosh(\lambda) \leq \exp\left(\frac{\lambda^2}{2}\right).$$

Par croissance de \ln , on a

$$\boxed{\forall \lambda \in \mathbb{R}, \varphi(\lambda) \leq \frac{\lambda^2}{2}}.$$

II.2. Comme $\lambda > 0$, on a l'égalité des événements

$$(S_k \geq t) = (\lambda S_k \geq \lambda t).$$

Par croissance de \exp qui est bijective,

$$(\lambda S_k \geq \lambda t) = (e^{\lambda S_k} \geq e^{\lambda t}).$$

On a donc

$$(S_k \geq t) = \left(\exp\left(\lambda \sum_{i=1}^k U_i\right) \geq e^{\lambda t} \right) = \left(\prod_{i=1}^k \exp(\lambda U_i) \geq e^{\lambda t} \right).$$

Par l'inégalité de Markov, puisque $e^{\lambda S_k}$ est une variable aléatoire réelle positive,

$$\begin{aligned} \mathbb{P}(S_k \geq t) &= \mathbb{P}(e^{\lambda S_k} \geq e^{\lambda t}) \\ &\leq \frac{\mathbb{E}[e^{\lambda S_k}]}{e^{\lambda t}} \\ &= e^{-\lambda t} \mathbb{E}\left[\prod_{i=1}^k e^{\lambda U_i}\right] \\ &\stackrel{*}{=} e^{-\lambda t} \prod_{i=1}^k \mathbb{E}[e^{\lambda U_i}] \\ &\stackrel{**}{=} e^{-\lambda t} \prod_{i=1}^k \underbrace{\mathbb{E}[e^{\lambda U_1}]}_{=\exp(\varphi(\lambda))} \\ &= \exp(k\varphi(\lambda) - \lambda t). \end{aligned}$$

1. pour la démontrer, il suffit de constater que $\frac{1}{(2n)!} \leq \frac{1}{2^n n!}$ pour tout $n \in \mathbb{N}$. On peut aussi faire une étude de fonction en étudiant $\lambda \mapsto \varphi(\lambda) - \lambda^2/2$ mais c'est un peu plus long.

où (\star) vient de l'indépendance de (U_1, \dots, U_k) et $(\star\star)$ vient du fait que les (U_1, \dots, U_k) ont la même loi donc $(e^{\lambda U_1}, \dots, e^{\lambda U_k})$ ont la même espérance. On a bien

$$\mathbb{P}(S_k \geq t) \leq \exp(k\varphi(\lambda) - \lambda t).$$

II.3. On a $\varphi(\lambda) \leq \frac{\lambda^2}{2}$ donc par croissance de exponentielle,

$$\mathbb{P}(S_k \geq t) \leq \exp\left(\frac{k\lambda^2}{2} - \lambda t\right).$$

Ceci étant vrai pour tout $\lambda > 0$, l'inégalité passe à l'infimum en

$$\mathbb{P}(S_k \geq t) \leq \inf_{\lambda > 0} \exp\left(\frac{k\lambda^2}{2} - \lambda t\right).$$

On minimise l'argument de l'exponentielle : c'est une fonction polynomiale de degré 2 de coefficient dominant positif donc atteint son minimum en $\frac{t}{k}$. Pour $\lambda = \frac{t}{k}$, on a

$$\exp\left(\frac{k\lambda^2}{2} - \lambda t\right) = \exp\left(\frac{k}{2} \frac{t^2}{k^2} - \frac{t^2}{k}\right) = \exp\left(-\frac{t^2}{2k}\right).$$

On a donc bien

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

II.4. • Comme C est une variable aléatoire, pour tout $i, j \in \llbracket 1, n \rrbracket$, $C_{i,j}$ est aussi une variable aléatoire (de Ω dans $\{-1, 1\}$). Ainsi, pour tout $x, y \in \{-1, 1\}$, $xyC_{i,j}$ est aussi une variable aléatoire de Ω dans $\{-1, 1\}$. En particulier,

$$(x_i y_j C_{i,j})_{1 \leq i, j \leq n} \text{ est une famille de } n^2 \text{ variables aléatoires à valeurs dans } \{-1, 1\}.$$

• Montrons qu'elles suivent toutes la loi uniforme. Soit $i, j \in \llbracket 1, n \rrbracket$. Soit $\varepsilon \in \{-1, 1\}$.

$$\mathbb{P}(x_i y_j C_{i,j} = \varepsilon) = \mathbb{P}(C_{i,j} = \varepsilon x_i y_j).$$

Or l'événement $(C_{i,j} = \alpha)$ est réalisé si, et seulement si, l'événement

$(C \text{ est une matrice où le coefficient en } (i, j) \text{ est } \alpha)$

est réalisé. Or, C est uniforme : le cardinal de l'ensemble des matrices ayant un coefficient fixé est 2^{n^2-1} donc

$$\mathbb{P}(x_i y_j C_{i,j} = \varepsilon) = \frac{2^{n^2-1}}{2^{n^2}} = \frac{1}{2} = \mathbb{P}(x_i y_j C_{i,j} = -\varepsilon)$$

donc pour tout $i, j \in \llbracket 1, n \rrbracket$, $x_i y_j C_{i,j}$ suit la loi uniforme dans $\{-1, 1\}$.

• Montrons qu'elles sont toutes indépendantes. Soit $A \subset \llbracket 1, n \rrbracket^2$. Soit $(\varepsilon_k)_{k \in A} \in \{-1, 1\}^A$ une famille d'éléments de $\{-1, 1\}$ indexée sur A . Alors l'événement

$$\left(\bigcap_{(i,j) \in A} (x_i y_j C_{i,j} = \varepsilon_{(i,j)}) \right)$$

est réalisé si, et seulement si, l'événement $(C \text{ est une matrice où ses coefficients en } A \text{ sont imposés par la condition souhaitée})$ est réalisé. Comme C est uniforme, il s'agit de compter le cardinal de l'ensemble des matrices ayant $\text{Card}(A)$ coefficients fixés : il y en a $2^{n^2 - \text{Card}(A)}$ matrices possibles.

Ainsi,

$$\mathbb{P}\left(\bigcap_{(i,j)\in A} (x_i y_j C_{i,j} = \varepsilon_{(i,j)})\right) = \frac{2^{n^2 - \text{Card}(A)}}{2^{n^2}} = \frac{1}{2^{\text{Card}(A)}}.$$

Or,

$$\prod_{(i,j)\in A} \mathbb{P}(x_i y_j C_{i,j} = \varepsilon_{(i,j)}) = \prod_{(i,j)\in A} \frac{1}{2} = \frac{1}{2^{\text{Card}(A)}}.$$

On a donc

$$\mathbb{P}\left(\bigcap_{(i,j)\in A} (x_i y_j C_{i,j} = \varepsilon_{(i,j)})\right) = \prod_{(i,j)\in A} \mathbb{P}(x_i y_j C_{i,j} = \varepsilon_{(i,j)})$$

et ce, pour tout $A \subset \llbracket 1, n \rrbracket^2$: les $(x_i y_j C_{i,j})_{1 \leq i, j \leq n}$ sont mutuellement indépendantes.

II.5. Soit $X = (x_i)_{1 \leq i \leq n}, Y = (y_j)_{1 \leq j \leq n} \in \{-1, 1\}^n$. Alors $X^T C Y = \sum_{i=1}^n \sum_{j=1}^n x_i y_j C_{i,j}$ est une somme de n^2 variables aléatoires indépendantes de loi uniforme dans $\{-1, 1\}$. On peut donc appliquer l'inégalité de Hoeffding (II.3) :

$$\mathbb{P}(X^T C Y \geq t n^{3/2}) \leq \exp\left(-\frac{(t n^{3/2})^2}{2(n^2)}\right) = \exp\left(-\frac{t^2 n}{2}\right).$$

Or, on a l'égalité des événements pour tout α

$$\left(\max\{X^T C Y : X, Y \in \{-1, 1\}^n\} \geq \alpha\right) = \left(\exists X, Y \in \{-1, 1\}^n, X^T C Y \geq \alpha\right) = \bigcup_{X, Y \in \{-1, 1\}^n} (X^T C Y \geq \alpha).$$

On a donc

$$\mathbb{P}(M(C) \geq t n^{3/2}) = \mathbb{P}\left(\bigcup_{X, Y \in \{-1, 1\}^n} (X^T C Y \geq t n^{3/2})\right)$$

et par σ -sous-additivité,

$$\begin{aligned} \mathbb{P}(M(C) \geq t n^{3/2}) &\leq \sum_{X, Y \in \{-1, 1\}^n} \mathbb{P}(X^T C Y \geq t n^{3/2}) \\ &\leq \exp\left(-\frac{t^2 n}{2}\right) \sum_{X, Y \in \{-1, 1\}^n} 1 \\ &\leq n^2 \exp\left(-\frac{t^2 n}{2}\right) \\ &= \exp\left(-\left(\frac{t^2}{2} - 2 \ln(2)\right) n\right). \end{aligned}$$

On a bien

$$\mathbb{P}(M(C) \geq t n^{3/2}) \leq \exp\left(-\left(\frac{t^2}{2} - 2 \ln(2)\right) n\right).$$

II.6. Commençons par l'indication. Soit $\varepsilon > 0$. Par la question II.5, on a

$$\mathbb{P}(M(C) \geq t n^{3/2}) \leq \exp\left(-\left(\frac{t^2}{2} - 2 \ln(2)\right) n\right)$$

pour tout $t \geq 0$: pour $t = 2\sqrt{\ln(2)} + \varepsilon$, on a

$$\mathbb{P}(M(C) \leq t n^{3/2}) \leq \exp\left(-n \left(\frac{4 \ln(2)}{2} + \frac{4\sqrt{\ln(2)}\varepsilon}{2} + \frac{\varepsilon^2}{2} - 2 \ln(2)\right)\right) = \exp\left(-n \underbrace{\left(\frac{\varepsilon^2 + 4\sqrt{\ln(2)}\varepsilon}{2}\right)}_{>0}\right) < 1$$

donc

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

Ainsi, il existe $\omega \in \Omega$ tel que $M(C)(\omega) \geq tn^{3/2}$ i.e. $M(C(\omega)) \geq tn^{3/2}$. Ainsi, pour tout $\varepsilon > 0$, il existe une matrice A vérifiant

$$M(A) \geq \left(2\sqrt{\ln(2)} + \varepsilon\right) n^{3/2}.$$

Attention ! A dépend de ε . En particulier,

$$\min\{M(A) : A \in \mathcal{M}_n(\{-1, 1\}) \leq M(A) \leq \left(2\sqrt{\ln(2)} + \varepsilon\right) n^{3/2}$$

(c'est bien un minimum qui existe car il y a un nombre fini d'élément à considérer) ce qui donne

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

L'inégalité passe à la limite quand ε tend vers 0 en

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

III Partie III

III.1. Soit $X = (x_1, \dots, x_n) \in \{-1, 1\}^n$. Alors

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

et

$$\forall i \in \llbracket 1, n \rrbracket, x_i \sum_{j=1}^n a_{i,j} y_j \leq \left| \sum_{j=1}^n a_{i,j} y_j \right|$$

avec égalité si, et seulement si, $x_i = \operatorname{sgn} \left(\sum_{j=1}^n a_{i,j} y_j \right)$. Ainsi, l'inégalité précédente donne que

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

et avec $x_i = \operatorname{sgn} \left(\sum_{j=1}^n a_{i,j} y_j \right)$ pour tout $i \in \llbracket 1, n \rrbracket$, on a

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

donc

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

III.2. Soit $i \in \llbracket 1, n \rrbracket$. Alors pour tout $j \in \llbracket 1, n \rrbracket$, $a_{i,j} Z_j$ suit une loi uniforme à valeurs dans $\{-1, 1\}$ en raisonnant comme à la question (II.4). On cherche donc à connaître la loi de S_k comme dans la partie II du sujet.

Ou bien on fait à la main, ou bien on peut remarquer qu'en notant $X_j = \frac{1}{2}(a_{i,j} Z_j + 1)$, X_j suit une loi

de Bernoulli de paramètre $\frac{1}{2}$. Ainsi, comme les Z_j sont indépendantes (on refait la même preuve qu'à la question II.4) et identiquement distribuées, les $(X_j)_{1 \leq j \leq n}$ les sont aussi. Ainsi, $\sum_{j=1}^n X_j =: T_n$ suit une loi binomiale de paramètre $\left(n, \frac{1}{2}\right)$. On en déduit que

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

On a bien

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

On en déduit que

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

donc

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

III.3.

(III.3.1) On a

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

On a bien

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

(III.3.2) On peut appliquer cette formule avec $m = \lfloor n/2 \rfloor$ ce qui donne

$$\sum_{k=0}^{\lfloor n/2 \rfloor} (n - 2k) \binom{n}{k} = n \binom{n-1}{\lfloor n/2 \rfloor}.$$

Si k vérifie $2k = n$, on a $\binom{n}{k} |n - 2k| = 0$ donc en écrivant $\llbracket 0, n \rrbracket = \{k \in \mathbb{N} : 2k \leq n\} \sqcup \{k \in \mathbb{N} :$

$2k > n$, on a

$$\begin{aligned}
 \sum_{k=0}^n \binom{n}{k} |n-2k| &= \sum_{2k \leq n} \binom{n}{k} |n-2k| + \sum_{2k > n} \binom{n}{k} |n-2k| \\
 &= \sum_{2k \leq n} \binom{n}{k} |n-2k| + \sum_{2k \geq n} \binom{n}{k} |n-2k| \\
 &= \sum_{2k \leq n} \binom{n}{k} |n-2k| + \underbrace{\sum_{2n-2k \geq n}}_{\Leftrightarrow 2k \leq n} \underbrace{\binom{n}{n-k}}_{=\binom{n}{k}} \underbrace{|n-2(n-k)|}_{=|n-2k|} \\
 &= 2 \sum_{2k \leq n} \binom{n}{k} |n-2k| \\
 &= 2 \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} (n-2k) \\
 &= 2n \binom{n-1}{\lfloor n/2 \rfloor}.
 \end{aligned}$$

Ainsi, par la question (III.2), on a exactement

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

III.4.

(III.4.1) Pour tout $\omega \in \Omega$, on a $g_A(Z(\omega)) \leq M(A)$ donc par croissance de l'espérance, on a

$$\mathbb{E}[g_A(Z)] \leq M(A).$$

Ainsi, par la question précédente, on a

$$\frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor n/2 \rfloor} \leq M(A).$$

La majoration est vraie pour tout $A \in \mathcal{M}_n(\{-1, 1\})$ donc l'inégalité passe à l'infimum : on a alors

$$M(n) \geq \frac{n^2}{2^{n-1}} \binom{n-1}{\lfloor n/2 \rfloor}.$$

(III.4.2) On a l'équivalent classique

$$\binom{2k}{k} \underset{k \rightarrow +\infty}{\sim} 4^k (k\pi)^{-1/2}.$$

En effet, par la formule de Stirling,

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

Ainsi, si n s'écrit $2k$, on a

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

Si n s'écrit $2k + 1$, on a

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

Puisque $k = \lfloor n/2 \rfloor \underset{n \rightarrow +\infty}{\sim} n/2$, on a

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

La constante C cherchée est $C = \sqrt{\frac{2}{\pi}}$ et la constante α cherchée est $\alpha = 3/2$.

On a un équivalent d'un minorant qui est du même ordre que le majorant. On veut donc montrer que C est inférieure à la constante trouvée pour la majoration *i.e.* vérifier

$$\sqrt{\frac{2}{\pi}} < 2\sqrt{\ln(2)}$$

ce qui est équivalent à demander $\frac{2}{\pi} < 4 \ln(2)$ *i.e.* $2 \ln(2)\pi > 1$. Or $2 \ln(2) = \ln(4) > \ln(e) = 1$, on a bien $2 \ln(2)\pi > 1$. On a

$$C = \sqrt{\frac{2}{\pi}} < 2\sqrt{\ln(2)}.$$

IV Partie IV

L'étude de la fonction $\Gamma : x \mapsto \int_0^{+\infty} t^{x-1} e^{-t} dt$ est très classique en CPGE. Ici, $I_n = \Gamma(n+1)$.

IV.1. On nous propose une récurrence, je vais plutôt faire un télescopage.

- Déjà, soit $n \in \mathbb{N}$. Alors $f : x \in \mathbb{R} \mapsto x^n e^{-x} \in \mathbb{R}$ est continue sur \mathbb{R}^+ .
- Par ailleurs, $\lim_{x \rightarrow +\infty} x^2 x^n e^{-x} = 0$ par croissances comparées. On en déduit que $x^n e^{-x} = o_{x \rightarrow +\infty}(x^{-2})$ donc par le critère de Riemann et par comparaison, f est intégrable au voisinage de $+\infty$.
- Ainsi, f est intégrable sur \mathbb{R}^+ donc I_n existe.

Soit $A > 0$. Alors

$$\int_0^A x^n e^{-x} dx = \underbrace{[-x^n e^{-x}]_0^A}_{=-A^n e^{-A} \xrightarrow{A \rightarrow +\infty} 0} + n \int_0^A x^{n-1} e^{-x} dx$$

donc l'égalité passe à la limite quand $A \rightarrow +\infty$ en

$$I_n = nI_{n-1}.$$

Comme I_n n'est pas nulle (puisque $x \mapsto x^n e^{-x}$ est positive continue sur \mathbb{R}^+ et non identiquement nulle), on a

$$\frac{I_n}{I_{n-1}} = n.$$

On en déduit que

$$\prod_{k=1}^n \frac{I_k}{I_{k-1}} = \frac{I_n}{I_0} = I_n = \prod_{k=1}^n k = n!$$

donc $\boxed{\forall n \in \mathbb{N}, I_n = n!}$.

IV.2. On réalise le changement de variable affine $u = 1 + \frac{x}{\sqrt{n}}$ ce qui donne

$$\left(\frac{n}{e}\right)^n \sqrt{n} \int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx = \left(\frac{n}{e}\right)^n \sqrt{n} \int_0^{+\infty} u^n e^{-n(u-1)} \sqrt{n} du = n^n \int_0^{+\infty} u^n e^{-nu} ndu.$$

On réalise le changement de variable affine $t = nu$ ce qui donne

$$n^n \int_0^{+\infty} u^n e^{-nu} ndu = n^n \int_0^{+\infty} t^n n^{-n} e^{-t} dt = \int_0^{+\infty} t^n e^{-t} dt = I_n.$$

On a donc bien

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

IV.3.

(IV.3.1) Si $(t, x) \in U$ et $x \leq 0$, alors $u = \frac{x}{t} \in]-1, 0]$. Alors

$$f(t, x) \leq -\frac{x^2}{2} \iff \ln(1 + u) - u \leq -\frac{u^2}{2}.$$

Posons $\varphi : u \in]-1, 0] \mapsto \ln(1 + u) - u + \frac{u^2}{2} \in \mathbb{R}$. Alors φ est dérivable et

$$\forall u \in]-1, 0], \varphi'(u) = \frac{1}{1+u} - 1 + u = \frac{1 - (1-u)(1+u)}{1+u} = \frac{u^2}{1+u} \geq 0.$$

Ainsi, φ est croissante donc

$$\forall u \in]-1, 0], \varphi(u) \leq \varphi(1) = 0$$

donc

$$\forall u \in]-1, 0], \ln(1 + u) - u \leq -\frac{u^2}{2}.$$

On en déduit donc avec $u = \frac{x}{t}$ que

$$\forall (t, x) \in U, x \leq 0, f(t, x) \leq -\frac{x^2}{2}.$$

(IV.3.2) Soit $x > 0, t \geq 1$. Alors

$$\partial_t f(t, x) = 2t \ln\left(1 + \frac{x}{t}\right) - t^2 \frac{x/t^2}{1 + \frac{x}{t}} - x = t \left(2 \ln\left(1 + \frac{x}{t}\right) - \frac{x/t}{1 + \frac{x}{t}} - \frac{x}{t}\right) = tF(x/t)$$

avec $F : u \in \mathbb{R}^+ \mapsto 2 \ln(1 + u) - \frac{u}{1 + u} - u \in \mathbb{R}$. On aimerait connaître le signe de F . F est dérivable et

$$\forall u \geq 0, F'(u) = \frac{2}{1+u} - \frac{1}{(1+u)^2} - 1 = \frac{2(1+u) - 1 - (1+u)^2}{(1+u)^2} = -\frac{u^2}{(1+u)^2} \leq 0$$

donc F décroît. Or $F(0) = 0$ donc F est négative. On en déduit que $\partial_t f(t, x)$ est négative pour tout $t \geq 1, x > 0$. On en déduit que pour tout $x > 0, t \mapsto f(t, x)$ décroît sur $[1, +\infty[$ donc

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

IV.4. On cherche la limite quand $n \rightarrow +\infty$ de

$$\int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx = \int_{-\infty}^{+\infty} \underbrace{\left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} \mathbf{1}_{]-\sqrt{n}, +\infty[}(x)}_{=: f_n(x)} dx.$$

- Pour tout $n \in \mathbb{N}$, f_n est continue par morceaux sur \mathbb{R} .
- On a $\forall x \in \mathbb{R}, \mathbb{1}_{]-\sqrt{n}, +\infty[}(x) \xrightarrow[n \rightarrow +\infty]{} 1$. Par ailleurs,

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

donc

$$f_n(x) = \exp\left(\sqrt{n}x - \frac{x^2}{2} + o_{n \rightarrow +\infty}(1)\right) e^{-\sqrt{n}x} (1 + o_{n \rightarrow +\infty}(1)) = e^{-x^2/2 + o_{x \rightarrow +\infty}(1)} \xrightarrow[n \rightarrow +\infty]{} e^{-x^2/2}.$$

- **Domination.** Soit $x \in \mathbb{R}, n \in \mathbb{N}^*$. Alors

$$|f_n(x)| \leq \exp\left(n \ln\left(1 + \frac{x}{\sqrt{n}}\right) - x\sqrt{n}\right) = \exp(f(\sqrt{n}, x)).$$

La question (IV.3.a) assure que

$$\forall x \leq 0, f(\sqrt{n}, x) \leq -\frac{x^2}{2}.$$

La question (IV.3.b) assure que

$$\forall x > 0, f(\sqrt{n}, x) \leq f(1, x).$$

Notons alors $\varphi(x) = -\frac{x^2}{2} \mathbb{1}_{x \leq 0} + f(1, x) \mathbb{1}_{x > 0}$. $\exp \circ \varphi$ est continue par morceaux, égale $x \mapsto \exp(-x^2/2)$ sur \mathbb{R}^- donc intégrable en $-\infty$, égale à $x \mapsto (1+x)^n e^{-x}$ sur \mathbb{R}^+ donc intégrable en $+\infty$. $\exp \circ \varphi$ est alors intégrable et

$$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}^*, |f_n(x)| \leq \exp(f(\sqrt{n}, x)) \leq \exp(\varphi(x)).$$

Ainsi, on a la domination souhaitée.

Par le théorème de convergence dominée,

$$\int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx = \int_{-\infty}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} \mathbb{1}_{]-\sqrt{n}, +\infty[}(x) dx \xrightarrow[n \rightarrow +\infty]{} \int_{-\infty}^{+\infty} e^{-x^2/2} dx = \sqrt{2\pi}.$$

Ainsi, par IV.2

$$\frac{I_n}{\left(\frac{n}{e}\right)^n \sqrt{n}} = \int_{-\sqrt{n}}^{+\infty} \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-x\sqrt{n}} dx \xrightarrow[n \rightarrow +\infty]{} \sqrt{2\pi}$$

ce qui donne bien par IV.1

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

V Partie V

V.1. Soit $Y = (y_1, \dots, y_n) \in \{-1, 1\}^n$ et $A = (a_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\{-1, 1\})$. On note $[AY]_i$ le i -ème coefficient de la matrice colonne AY . On a alors

$$[AY]_i = \sum_{j=1}^n \underbrace{a_{i,j} y_j}_{\in \{-1, 1\}} \in \llbracket -n, n \rrbracket.$$

Ainsi, pour tout $X = (x_1, \dots, x_n) \in \{-1, 1\}^n$, on a $X^T AY$ qui est une somme de termes de la forme $x_i \alpha_i$ avec $x_i \in \{-1, 1\}$ et $\alpha_i \in \llbracket -n, n \rrbracket$.

Montrons par récurrence sur k que si on a $(\alpha_1, \dots, \alpha_k) \in [-C, C]^k$, alors il existe $x_1, \dots, x_k \in \{-1, 1\}^k$ tel que

$$\sum_{i=1}^k x_i \alpha_i \in [-C, C].$$

Avant cela, montrons un lemme. Soit $C > 0$. Si a, b sont deux réels tels que $|a|, |b| \leq C$, alors $|a - b| \leq C$ ou $|a + b| \leq C$.

Démonstration. Sans perdre de généralités, on peut supposer que $a \leq b$. Si $|b - a| > C$, alors $b > a + C$ et comme $b \leq C$, nécessairement, $a < 0$ donc $b + a \leq C$. Par ailleurs, $b + a > 2a + C \geq -2C + C \geq -C$ donc $|b + a| \leq C$. Ainsi, soit $|b - a| \leq C$, soit $|b + a| \leq C$. \square

- Pour $k = 1$, il n'y a rien à faire.
- Supposons le résultat acquis au rang k . Soit $\alpha_1, \dots, \alpha_{k+1} \in [-C, C]^{k+1}$. Alors $\alpha_1, \dots, \alpha_k \in [-C, C]^k$ donc par hypothèse de récurrence, on dispose de $x_1, \dots, x_k \in \{-1, 1\}^k$ tel que

$$\alpha = \sum_{i=1}^k x_i \alpha_i \in [-C, C].$$

Comme α et $\alpha_{k+1} \in [-C, C]$, par le lemme, il existe $x_{k+1} \in \{-1, 1\}$ tel que $|\alpha + x_{k+1} \alpha_{k+1}| \leq C$. On en déduit que

$$\sum_{i=1}^{k+1} x_i \alpha_i \in [-C, C]$$

ce qui conclut l'hérédité.

- Par le principe de récurrence, on a le résultat souhaité.

Soit donc $(x_1, \dots, x_n) \in \{-1, 1\}^n$ tel que

$$\sum_{i=1}^n x_i [AY]_i \in [-n, n].$$

Alors $X = (x_1, \dots, x_n) \in \{-1, 1\}^n$ satisfait $|X^T AY| \leq n$. En particulier,

$$\min\{|Z^T AY| : Z \in \{-1, 1\}^n\} \leq |X^T AY| \leq n$$

et comme $\{|Z^T AY| : Z \in \{-1, 1\}^n\} \subset S(A) \cap \mathbb{N}$, on a

$$m(A) \leq \min\{|Z^T AY| : Z \in \{-1, 1\}^n\} \leq n.$$

V.2. Posons $t = \sqrt{2n \ln(2n)} + \varepsilon$. Notons $A = (a_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\{-1, 1\})$. Soit Z une variable aléatoire uniforme de Ω dans $\{-1, 1\}^n$. Notons Z_i sa i -ème coordonnée. Pour tout $i \in \llbracket 1, n \rrbracket$, comme à la question (III.2), $a_{i,j} Z_j$ suit une loi uniforme sur $\{-1, 1\}$ et les $(a_{i,j} Z_j)_{1 \leq j \leq n}$ sont indépendantes. En notant $S_{i,n} = \sum_{j=1}^n a_{i,j} Z_j$, on est dans le cadre de la partie II. On peut utiliser l'inégalité de Hoeffding :

$$\mathbb{P}(S_{i,n} \geq t) \leq \exp\left(-\frac{t^2}{2n}\right).$$

Par ailleurs, on a l'égalité des événements

$$(|S_{i,n}| \geq t) = (S_{i,n} \geq t) \cup (S_{i,n} \leq -t)$$

donc

$$\mathbb{P}(|S_{i,n}| \geq t) \leq \mathbb{P}(S_{i,n} \geq t) + \mathbb{P}(S_{i,n} \leq -t)$$

où $R_{i,n} = \sum_{j=1}^n (-a_{i,j}Z_j)$ et les $(-a_{i,j}Z_j)_{1 \leq j \leq n}$ sont indépendantes et suivent toutes la loi uniforme sur $\{-1, 1\}$ donc on peut aussi appliquer l'inégalité de Hoeffding sur $R_{i,n}$. On obtient alors

$$\mathbb{P}(|S_{i,n}| \geq t) \leq 2 \exp\left(-\frac{t^2}{2n}\right).$$

On veut appliquer les mêmes techniques que la question précédente : pour cela, on veut $\omega \in \Omega$ tel que pour tout $i \in \llbracket 1, n \rrbracket$, $|S_{i,n}(\omega)| \leq t$. On a

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

et

$$2n \exp\left(-\frac{t^2}{2n}\right) = 2n \exp\left(-\frac{t^2}{2n}\right) = \exp\left(-\frac{t^2}{2n} + \ln(2n)\right) = \exp\left(\frac{-t^2 + 2n \ln(2n)}{2n}\right) < 1.$$

puisque $t^2 = (\sqrt{2n \ln(2n)} + \varepsilon)^2 > \sqrt{2n \ln(2n)}^2 = 2n \ln(2n)$. Ainsi, en passant au complémentaire,

$$\mathbb{P}(\forall i \in \llbracket 1, n \rrbracket, |S_{i,n}| \leq t) > 0$$

donc il existe $\omega \in \Omega$ tel que $\forall i \in \llbracket 1, n \rrbracket, \left| \sum_{j=1}^n a_{i,j}Z_j(\omega) \right| \leq t$.

A la question précédente, on a montré que si on a $(\alpha_1, \dots, \alpha_k) \in [-C, C]^k$, alors il existe $x_1, \dots, x_k \in \{-1, 1\}^k$ tel que

$$\sum_{i=1}^k x_i \alpha_i \in [-C, C].$$

On applique donc ce résultat pour obtenir un vecteur $X \in \{-1, 1\}^n$ tel que $|X^T AZ(\omega)| \leq t$. En particulier,

$$\min\{|U^T AY| : U \in \{-1, 1\}^n\} \leq |X^T AZ(\omega)| \leq t$$

donc comme à la question précédente,

$$m(A) \leq \min\{|U^T AY| : Z \in \{-1, 1\}^n\} \leq t = \sqrt{2n \ln(2n)} + \varepsilon.$$

L'inégalité $m(A) \leq \sqrt{2n \ln(2n)} + \varepsilon$ est vraie pour tout $\varepsilon > 0$ donc elle passe à la limite en

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

FIN DU SUJET
