CCS PSI MATHS1 2022

Rémi Crétois

version du 6 mai 2022

I Partie I

I.A Quelques résultats préliminaires

Q 1. — Soit $A, B \in \mathcal{M}_n(\mathbb{R})$ et $\lambda \in \mathbb{R}$.

$$\begin{aligned}
\operatorname{tr}(\lambda A + B) &= \sum_{k=1}^{n} [\lambda A + B]_{kk} \\
&= \sum_{k=1}^{n} \lambda [A]_{kk} + [B]_{kk} \\
&= \lambda \sum_{k=1}^{n} [A]_{kk} + \sum_{k=1}^{n} [B]_{kk} \\
&= \lambda \operatorname{tr}(A) + \operatorname{tr}(B)
\end{aligned}$$

donc $\boxed{\text{tr est une forme linéaire}}$.

— Soit $A, B \in \mathcal{M}_n(\mathbb{R})$.

$$\begin{aligned}
\operatorname{tr}(AB) &= \sum_{k=1}^{n} [AB]_{kk} \\
&= \sum_{k=1}^{n} \sum_{i=1}^{n} [A]_{ki} [B]_{ik} \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} [B]_{ik} [A]_{ki} \\
&= \sum_{i=1}^{n} [BA]_{ii}
\end{aligned}$$

donc $\boxed{\operatorname{tr}(AB) = \operatorname{tr}(BA)}$.

Q 2. — Symétrie : soit $A, B \in \mathcal{M}_n(\mathbb{R})$:

$$\operatorname{tr}(A^\top B) = \operatorname{tr}\left((A^\top B)^\top\right) = \operatorname{tr}(B^\top A)$$

car la trace d'une matrice est égale à la trace de sa transposée.

— Bilinéarité : soit $A, B, C \in \mathcal{M}_n(\mathbb{R})$ et $\lambda \in \mathbb{R}$:

$$\operatorname{tr}(A^\top(\lambda B + C)) = \operatorname{tr}(\lambda A^\top B + A^\top C) = \lambda \operatorname{tr}(A^\top B) + \operatorname{tr}(A^\top C)$$

par linéarité de la trace. L'application est donc linéaire à droite, et par symétrie, elle est bilinéaire.

— Positivité et définition : soit $A \in \mathcal{M}_n(\mathbb{R})$, alors

$$\begin{aligned}\operatorname{tr}(A^\top A) &= \sum_{k=1}^{n} [A^\top A]_{kk} \\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} [A^\top]_{ki}[A]_{ik} \\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} ([A]_{ik})^2\end{aligned}$$

Comme A est à coefficients réels, $\operatorname{tr}(A^\top A) \geqslant 0$. De plus, $\operatorname{tr}(A^\top A) = 0$ si et seulement si tous les termes de la somme sont nuls : $\operatorname{tr}(A^\top A) = 0 \iff A = 0_n$.

L'application donnée $\boxed{\text{est bien un produit scalaire sur } \mathcal{M}_n(\mathbb{R})}$.

Q 3. Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^\top A = 0_n$. En particulier, $\boxed{\operatorname{tr}(A^\top A) = 0, \text{ donc } A = 0_n}$ par définition du produit scalaire.

I.B Quelques propriétés de $\mathcal{N}_n$

Q 4. Soit $A \in \mathcal{N}_n$. Alors il existe $k \in \mathbb{N}^*$ tel que $A^k = 0_n$. En particulier, A n'est pas inversible. Ainsi, le noyau de A n'est pas réduit au vecteur nul : il existe $X \in \mathcal{M}_{n,1}(\mathbb{R})$ non nul tel que $AX = 0 \cdot X$, donc $\boxed{0 \text{ est valeur propre de } A}$.
Soit $\lambda \in \mathbb{R}$ une valeur propre de A et soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$ un vecteur propre associé. Alors $AX = \lambda X$, et par récurrence immédiate, $A^k X = \lambda^k X$. Donc $\lambda^k X = 0_n$. Comme X est non nul, $\lambda^k = 0$, donc $\lambda = 0$. $\boxed{\text{La seule valeur propre de } A \text{ est donc } 0}$.

Q 5. Soit $A \in \mathcal{N}_n$. D'après la question précédente, A n'est pas inversible, donc $\boxed{\det(A) = 0}$.
D'autre part A est trigonalisable sur $\mathbb{C}$: il existe $P \in \mathcal{M}_n(\mathbb{C})$ inversible telle que $T = PAP^{-1}$ est triangulaire supérieure. En outre, les coefficients diagonaux de T sont les valeurs propres de A : ils sont donc tous nuls d'après la question précédente. Ainsi,

$$\operatorname{tr}(A) = \operatorname{tr}(P^{-1}TP) = \operatorname{tr}(PP^{-1}T) = \operatorname{tr}(T) = 0.$$

$\boxed{\text{Donc } \operatorname{tr}(A) = 0}$.

Q 6. Soit $M \in \mathcal{N}_n$. Alors il existe $k \in \mathbb{N}^*$ tel que $M^k = 0_n$. Puis, pour tout $\ell \geqslant k$, $M^\ell = M^k M^{\ell-k} = 0_n$. Donc $(M^2)^k = M^{2k} = 0_n$. $\boxed{\text{La matrice } M^2 \text{ est nilpotente}}$.

Q 7. Soit $M, N \in \mathcal{N}_n$ telles que $MN = NM$. Il existe $k, k' \in \mathbb{N}^*$ avec $M^k = N^{k'} = 0_n$. Alors $(MN)^{k+k'} = M^{k+k'}N^{k+k'}$ car M et N commutent, puis $M^{k+k'} = N^{k+k'} = 0_n$. Donc $\boxed{MN \text{ est nilpotente}}$.
On peut d'autre part appliquer la formule du binome de Newton :

$$(M+N)^{k+k'} = \sum_{i=0}^{k+k'} \binom{k+k'}{i} M^i N^{k+k'-i}$$

Or, pour $i < k$, $N^{k+k'-i} = N^{k'}N^{k-i} = 0_n$ et pour $i \geqslant k$, $M^k = 0_n$. Tous les termes de la somme précédente sont nuls : $(M+N)^{k+k'} = 0_n$. $\boxed{\text{La matrice } M+N \text{ est nilpotente}}$.

Q 8. Soit $M, N \in \mathcal{N}_n$ telles que $M + N \in \mathcal{N}_n$. On a :

$$(M+N)^2 - M^2 - N^2 = MN + NM.$$

Or, M^2, N^2 et $(M+N)^2$ sont nilpotentes d'après 6. D'après la question 5, $\operatorname{tr}((M+N)^2) = \operatorname{tr}(M^2) = \operatorname{tr}(N^2) = 0$, donc par linéarité, $\operatorname{tr}(MN+NM) = 0$. Or $\operatorname{tr}(MN+NM) = 2\operatorname{tr}(MN)$. D'où $\boxed{\operatorname{tr}(MN) = 0}$.

Q 9. Soit $M \in \mathcal{M}_2(\mathbb{R})$. D'après la question 5, si M est nilpotente, alors $\operatorname{tr}(M) = \det(M) = 0$.
Réciproquement, supposons que $\operatorname{tr}(M) = \det(M) = 0$. Alors $\chi_M(X) = X^2 - \operatorname{tr}(M)X + \det(M) = X^2$. D'après le théorème de Cayley-Hamilton, $\chi_M(M) = 0_n$. D'où $M^2 = 0_2$ et M est nilpotente.
Ainsi, $\boxed{M \in \mathcal{N}_2 \iff \det(M) = \operatorname{tr}(M) = 0}$.

Q 10. Soit $M \in \mathcal{M}_n(\mathbb{R})$ nilpotente et symétrique. D'après la question 4, la seule valeur propre de M est 0. Comme M est symétrique réelle, elle est diagonalisable. Donc M est semblable à la matrice nulle. Ainsi, $\boxed{M = 0_n}$.

Q 11. Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice nilpotente et antisymétrique. On a $A^\top A = -A^2$. Comme A est nilpotente, A^2 aussi, puis $-A^2$ aussi. Ainsi, $A^\top A$ est nilpotente.
Or $(A^\top A)^\top = A^\top A$, donc $A^\top A$ est symétrique.
D'après la question précédente, $\boxed{A^\top A = 0_n}$.
D'après la question 3, $\boxed{A = 0_n}$.

Q 12. On peut prendre par exemple une matrice diagonale : $M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$. On a $\det(M) = \operatorname{tr}(M) = 0$. Par contre, si $k \in \mathbb{N}$ est pair, $M^k = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et si k est impair, $M^k = M$. Donc M n'est pas nilpotente.
On peut donner un exemple pour tout $n \geqslant 3$ en prenant $M = \operatorname{diag}(0, \dots, 0, 1, -1)$.

II Matrices aléatoires à coefficients dans $\{-1, 1\}$

II.A Quelques résultats algébriques

Q 13. Soit $i \in [\![1, n]\!]$. Alors $\boxed{E_i = \frac{1}{2}V - \frac{1}{2}(V - 2E_i)}$.
Or pour tout $i \in [\![1, n]\!]$, $V - 2E_i \in \mathcal{V}_{n,1}$ et $V \in \mathcal{V}_{n,1}$, donc $E_i \in \operatorname{Vect}(\mathcal{V}_{n,1})$. Comme $(E_1, \dots, E_n)$ engendre $\mathcal{M}_{n,1}(\mathbb{R})$, $\boxed{\mathcal{M}_{n,1}(\mathbb{R}) = \operatorname{Vect}(\mathcal{V}_{n,1})}$

Q 14. — Unicité : soit $i, j \in [\![1, n-1]\!]$ tels que :

$$\begin{cases} (C_1, \dots, C_i) \text{ est libre} \\ C_{i+1} \in \operatorname{Vect}(C_1, \dots, C_i) \end{cases} \quad \text{et} \quad \begin{cases} (C_1, \dots, C_j) \text{ est libre} \\ C_{j+1} \in \operatorname{Vect}(C_1, \dots, C_j) \end{cases}$$

Alors $(C_1, \dots, C_{i+1})$ est liée, donc pour tout $k \geqslant i+1$, $(C_1, \dots, C_k)$ est liée. En particulier, $j \leqslant i$. De même, $i \leqslant j$. Donc $\boxed{i = j}$.

— Existence : soit $A = \{j \in [\![1, n-1]\!], (C_1, \dots, C_j) \text{ est libre}\}$. L'ensemble A est non vide car C_1 est non nulle. Prenons donc $j_0 = \max(A) \in [\![1, n-1]\!]$. En particulier, $(C_1, \dots, C_{j_0})$ est libre.
De plus, si $j_0 = n-1$, alors $(C_1, \dots, C_{j_0+1}) = (C_1, \dots, C_n)$ est liée par hypothèse.
Si $j_0 < n-1$, alors $j_0 + 1 \in [\![1, n-1]\!]$ donc $(C_1, \dots, C_{j_0+1})$ est liée par maximalité de j_0.
Ainsi, $\boxed{j_0 \text{ vérifie les conditions voulues}}$.

Q 15. Ça ressemble à une projection sur un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{R})$ engendré par d vecteurs de la base canonique.
Plus précisément, comme $(U_1, \dots, U_d)$ est libre, on peut compléter la famille avec $n-d$ vecteurs de

la base canonique pour obtenir une base de $\mathcal{M}_{n,1}(\mathbb{R})$. Notons $1 \leqslant i_1 < \cdots < i_d \leqslant n$ les indices des vecteurs de la base canonique non utilisés pour cette complétion. Alors, H et $\mathrm{Vect}((E_i)_{i\notin\{i_1,\ldots,i_d\}})$ sont supplémentaires dans $\mathcal{M}_{n,1}(\mathbb{R})$.
Posons alors $\varphi : H \to \mathcal{M}_{d,1}(\mathbb{R})$ telle que $\varphi(x_1,\ldots,x_n) = (x_{i_1},\ldots,x_{i_d})$. C'est une application linéaire. Vérifions que φ est injective : soit $(x_1,\ldots,x_n) \in \ker(\varphi)$. Alors $x_{i_1} = \cdots = x_{i_d} = 0$. Ainsi, $(x_1,\ldots,x_n) \in \mathrm{Vect}((E_i)_{i\notin\{i_1,\ldots,i_d\}}) \cap H$, donc $(x_1,\ldots,x_n) = 0_n$.
Comme $\dim(H) = \dim(\mathcal{M}_{d,1}(\mathbb{R}))$, $\boxed{\varphi \text{ est donc un isomorphisme}}$.

Q 16. Comme $\mathcal{W}$ est de dimension d, il existe une base $(U_1,\ldots,U_d)$ de $\mathcal{W}$. D'après la question 15, il existe $1 \leqslant i_1 < \cdots < i_d \leqslant n$ tels que

$$\left|\begin{array}{cccc} \varphi : & \mathcal{W} & \to & \mathcal{M}_{d,1}(\mathbb{R}) \\ & \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{array}\right.$$

est une bijection. Or $\varphi(\mathcal{W} \cap \mathcal{V}_{n,1}) \subset \mathcal{V}_{d,1}$. Donc

$$\boxed{\mathrm{card}(\mathcal{W} \cap \mathcal{V}_{n,1}) = \mathrm{card}(\varphi(\mathcal{W} \cap \mathcal{V}_{n,1})) \leqslant \mathrm{card}(\mathcal{V}_{d,1}) = 2^d}$$

II.B Une loi de probabilité

Q 17. La variable $\dfrac{1}{2}(X+1)$ suit la $\boxed{\text{loi de Bernoulli de paramètre } \dfrac{1}{2}}$.

Q 18. Soit X qui suit la loi $\mathcal{R}$.

$$\mathbb{E}(X) = -1\cdot\mathbb{P}(X=-1) + 1\cdot\mathbb{P}(X=1) = 0 \quad \text{ et } \quad \mathbb{E}(X^2) = (-1)^2\cdot\mathbb{P}(X=-1) + 1^2\cdots\mathbb{P}(X=1) = 1$$

Donc $\mathbb{V}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = 1$. Donc $\boxed{\mathbb{E}(X) = 0 \text{ et } \mathbb{V}(X) = 1}$.

Q 19. Soient X et Y suivant $\mathcal{R}$ et indépendantes. Notons $Z = XY$. Alors Z prend les valeurs 1 et -1. De plus,

$$\mathbb{P}(Z=1) = \mathbb{P}(X=1, Y=1) + \mathbb{P}(X=-1, Y=-1) = \mathbb{P}(X=1)\mathbb{P}(Y=1) + \mathbb{P}(X=-1)\mathbb{P}(Y=-1) = \frac{1}{2}$$

par indépendance. Donc $\boxed{Z \text{ suit aussi la loi } \mathcal{R}}$.

II.C Un premier procédé de génération de matrices aléatoires à coefficients dans $\{-1, 1\}$

Q 20. Par linéarité de l'espérance,

$$\mathbb{E}(\tau_n) = \mathbb{E}\left(\sum_{i=1}^n m_{i,i}\right) = \sum_{i=1}^n \mathbb{E}(m_{i,i}).$$

Comme les $m_{i,i}$ ($i \in [\![1,n]\!]$) suivent la loi $\mathcal{R}$, leur espérance est nulle (question 18). Donc $\boxed{\mathbb{E}(\tau_n) = 0}$.
Comme les $m_{i,i}$ ($i \in [\![1,n]\!]$) sont mutuellement indépendantes,

$$\mathbb{V}(\tau_n) = \sum_{i=1}^n \mathbb{V}(m_{i,i}).$$

D'après la question 18, on obtient $\boxed{\mathbb{V}(\tau_n) = n}$.

Q 21. En développant le déterminant par rapport à la première ligne :

$$\delta_n = \sum_{j=1}^{n} m_{1,j}\Delta_{1,j}$$

où $\Delta_{1,1},\dots,\Delta_{1,n}$ sont les mineurs de la matrice M_n. D'après le lemme des coalitions, pour tout $j \in [\![1,n]\!]$, $m_{1,j}$ et $\Delta_{1,j}$ sont indépendantes. Donc

$$\mathbb{E}(\delta_n) = \sum_{j=1}^{n} \underbrace{\mathbb{E}(m_{1,j})}_{=0}\mathbb{E}(\Delta_{1,j}).$$

Ainsi, $\boxed{\mathbb{E}(\delta_n)=0}$.

Q 22. Montrons par récurrence la propriété $\mathcal{P}_n$: pour toute matrice aléatoire N_n de taille n dont les coefficients sont mutuellement indépendants et suivent la loi $\mathcal{R}$, $\mathbb{V}(\det(N_n)) = n!$.

— Initialisation : pour $n=1$, soit N_1 une matrice aléatoire de taille dont le coefficient suit $\mathcal{R}$. Alors $\mathbb{V}(\det(N_1)) = \mathbb{V}(n_{1,1}) = 1$ d'après la question 18. Donc $\mathcal{P}_1$ est vraie.

— Hérédité : soit $n \geqslant 1$ telle que $\mathcal{P}_n$ est vraie. Soit N_{n+1} une matrice de taille $n+1$ dont les coefficients sont mutuellement indépendants et suivent la loi $\mathcal{R}$. En développant par rapport à la première ligne :

$$\det(N_{n+1}) = \sum_{j=1}^{n+1} n_{1,j}\Delta_{1,j},$$

où $\Delta_{1,j}$ sont les mineurs de N_{n+1}. Puis,

$$\mathbb{E}(\det(N_{n+1})^2) = \mathbb{E}\left(\sum_{1\leqslant j,k\leqslant n+1} n_{1,j}n_{1,k}\Delta_{1,j}\Delta_{1,k}\right) = \sum_{1\leqslant j,k\leqslant n+1} \mathbb{E}(n_{1,j}n_{1,k}\Delta_{1,j}\Delta_{1,k})$$

par linéarité de l'espérance. D'après le lemme des coalitions, $n_{1,j}n_{1,k}$ et $\Delta_{1,j}\Delta_{1,k}$ sont indépendantes, et d'après la question 19, si $j \neq k$, $n_{1,j}n_{1,k}$ suit la loi $\mathcal{R}$. Donc

$$\mathbb{E}(\det(N_{n+1})^2) = \sum_{1\leqslant j,k\leqslant n+1} \underbrace{\mathbb{E}(n_{1,j}n_{1,k})}_{=0 \text{ si } j\neq k}\mathbb{E}(\Delta_{1,j}\Delta_{1,k}) = \sum_{j=1}^{n+1}\mathbb{E}(n_{1,j}^2)\mathbb{E}(\Delta_{1,j}^2).$$

De plus, pour tout $j \in [\![1,n]\!]$, $n_{1,j}^2$ vaut 1 avec probabilité 1 et d'après la question 21, $\mathbb{E}(\Delta_{1,j}^2) = \mathbb{V}(\Delta_{1,j})$. Par hypothèse de récurrence, $\mathbb{V}(\Delta_{1,j}) = n!$. Donc

$$\mathbb{E}(\det(N_{n+1})^2) = \sum_{j=1}^{n+1} n! = (n+1)!$$

Enfin, d'après la question 21, $\mathbb{V}(\det(N_{n+1})) = \mathbb{E}(\det(N_{n+1})^2)$.
Ainsi, la propriété $\mathcal{P}_{n+1}$ est vraie.

D'après le principe de récurrence, on en déduit que $\boxed{\delta_n = n!}$.

Q 23. D'après la question 9, $(M_2 \in \mathcal{N}_2) = (\delta_2 = 0) \cap (\tau_2 = 0)$. Donc d'après la formule des probabilités composées :

$$\mathbb{P}(M_2 \in \mathcal{N}_2) = \mathbb{P}(\tau_2 = 0)\mathbb{P}_{(\tau_2=0)}(\delta_2 = 0)$$

Or, $\mathbb{P}_{(\tau_2=0)}(\delta_2 = 0) = \mathbb{P}(-m_{1,1}^2 - m_{1,2}m_{2,1} = 0) = \mathbb{P}(m_{1,2}m_{2,1} = -1) = \dfrac{1}{2}$ d'après la question 19. D'autre part, $\mathbb{P}(\tau_2 = 0) = \mathbb{P}(m_{1,1} = -m_{2,2}) = \mathbb{P}(m_{1,1} = 1, m_{2,2} = -1) + \mathbb{P}(m_{1,1} = -1, m_{2,2} = 1) = \dfrac{1}{2}$ par indépendance. Ainsi, $\boxed{\mathbb{P}(M_2 \in \mathcal{N}_2) = \dfrac{1}{4}}$.

Q 24. $\mathbb{P}(M_2 \in \mathcal{G}\ell_2(\mathbb{R})) = \mathbb{P}(\delta_2 \neq 0) = 1 - \mathbb{P}(\delta_2 = 0)$. Or

$$\mathbb{P}(\delta_2 = 0) = \mathbb{P}(m_{1,1}m_{2,2} = m_{2,1}m_{1,2}).$$

D'après 19, les variables $a = m_{1,1}m_{2,2}$ et $b = m_{2,1}m_{1,2}$ suivent la loi $\mathcal{R}$. Elles sont de plus indépendantes d'après le lemme des coalitions. Donc

$$\mathbb{P}(\delta_2 = 0) = \mathbb{P}(a = 1, b = 1) + \mathbb{P}(a = -1, b = -1) = \mathbb{P}(a = 1)\mathbb{P}(b = 1) + \mathbb{P}(a = -1)\mathbb{P}(b = -1) = \frac{1}{2}.$$

Ainsi, $\boxed{\mathbb{P}(M_2 \in \mathcal{G}\ell_2(\mathbb{R})) = \frac{1}{2}}$.

II.D Une généralisation

Q 25. Comme les variables $c_1, \dots, c_n$ sont mutuellement indépendantes, pour tout $(\varepsilon_1, \dots, \varepsilon_n) \in \{-1, 1\}^n$,

$$\boxed{\mathbb{P}((c_1 = \varepsilon_1) \cap \dots \cap (c_n = \varepsilon_n)) = \mathbb{P}(c_1 = \varepsilon_1) \cdots \mathbb{P}(c_n = \varepsilon_n) = \frac{1}{2^n}.}$$

Q 26. Soit $\omega \in \Omega$. Supposons que $(C(\omega), C'(\omega))$ est liée. Il existe alors $\alpha, \alpha' \in \mathbb{R}$ tels que $\alpha C(\omega) + \alpha' C'(\omega) = 0_n$. Comme $C(\omega)$ est non nul, α' est non nul, donc $C'(\omega) = -\dfrac{\alpha}{\alpha'}C(\omega)$. On pose $\varepsilon = -\dfrac{\alpha}{\alpha'}$, de sorte que $C'(\omega) = \varepsilon C(\omega)$. Puis, comme $c_1'(\omega) = \varepsilon c_1(\omega)$ et $c_1(\omega) \neq 0$, $\varepsilon = \dfrac{c_1'(\omega)}{c_1(\omega)} \in \{-1, 1\}$.
Réciproquement, s'il existe $\varepsilon \in \{-1, 1\}$ tel que $C'(\omega) = \varepsilon C(\omega)$ alors $(C(\omega), C'(\omega))$ est bien liée.
Ainsi, $\boxed{\text{pour tout } \omega \in \Omega,\ (C(\omega), C'(\omega)) \text{ est liée ssi il existe } \varepsilon \in \{-1,1\} \text{ tel que } C'(\omega) = \varepsilon C(\omega)}$.

Q 27. D'après la question précédente,

$$\mathbb{P}((C, C') \text{ est liée}) = \mathbb{P}((C = C') \cup (C = -C')) = \mathbb{P}(C = C') + \mathbb{P}(C = -C').$$

Or

$$\mathbb{P}(C = C') = \sum_{(\varepsilon_1, \dots, \varepsilon_n) \in \{-1,1\}^n} \mathbb{P}(c_1 = \varepsilon_1, c_1' = \varepsilon_1, \dots, c_n = \varepsilon_n, c_n' = \varepsilon_n)$$

D'après la question 25 et par indépendance,

$$\mathbb{P}(C = C') = \sum_{(\varepsilon_1, \dots, \varepsilon_n) \in \{-1,1\}^n} \frac{1}{2^{2n}} = \frac{1}{2^n}.$$

De la même façon, on trouve $\mathbb{P}(C = -C') = \dfrac{1}{2^n}$. Donc $\boxed{\mathbb{P}((C'C') \text{ est liée}) = \dfrac{1}{2^{n-1}}}$.

Q 28. Soit $\omega \in \Omega$. D'après la question 14,
- soit $(C_1(\omega), \dots, C_n(\omega))$ est libre et alors $\omega \in R_n$ et $\omega \notin R_k$ pour $k \in [\![1, n-1]\!]$,
- soit il existe un unique $j \in [\![1, n-1]\!]$ tel que $\omega \in R_j$.

Ainsi, $\Omega = \displaystyle\bigcup_{j=1}^{n} R_j$ et l'union est disjointe. $\boxed{\text{Donc } (R_1, \dots, R_n) \text{ est un système complet d'évènements}}$.

Q 29. Une matrice M est inversible si et seulement si la famille de ses vecteurs colonnes est libre. Donc $(M_n \notin \mathcal{G}\ell_n(\mathbb{R})) = ((C_1, \dots, C_n) \text{ est liée})$. D'après la formule des probabilités totales appliquée avec le système complet d'évènements $(R_1, \dots, R_n)$:

$$\mathbb{P}(M_n \notin \mathcal{G}\ell_n(\mathbb{R})) = \sum_{j=1}^{n} \mathbb{P}\left(((C_1, \dots, C_n) \text{ est liée}) \cap R_j\right).$$

Or, $\mathbb{P}\left(((C_1,\dots,C_n) \text{ est liée}) \cap R_n\right) = 0$ et pour $j \in [\![1, n-1]\!]$, $(((C_1,\dots,C_n) \text{ est liée}) \cap R_j) = R_j \subset (C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j))$. Par croissance de la probabilité :

$$\boxed{\mathbb{P}(M_n \notin \mathcal{G}\ell_n(\mathbb{R})) \leqslant \sum_{j=1}^{n-1} \mathbb{P}(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)).}$$

Q 30. Soit $j \in [\![1, n-1]\!]$. La famille $((C_1 = v_1) \cap \dots \cap (C_j = v_j))_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j}$ est un système complet d'évènements. D'après la formule des probabilités totales :

$$\begin{aligned}
\mathbb{P}\left(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)\right) &= \sum_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j} \mathbb{P}\left((C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)) \cap ((C_1 = v_1) \cap \dots \cap (C_j = v_j))\right) \\
&= \sum_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j} \mathbb{P}_{((C_1 = v_1) \cap \dots \cap (C_j = v_j))}\left(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)\right) \times \\
&\qquad \mathbb{P}\left((C_1 = v_1) \cap \dots \cap (C_j = v_j)\right)
\end{aligned}$$

d'après la formule des probabilités composées. Or

$$\mathbb{P}_{((C_1 = v_1) \cap \dots \cap (C_j = v_j))}\left(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)\right) = \mathbb{P}\left(C_{j+1} \in \mathrm{Vect}(v_1,\dots,v_j)\right).$$

Donc

$$\boxed{\mathbb{P}\left(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)\right) = \sum_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j} \mathbb{P}\left(C_{j+1} \in \mathrm{Vect}(v_1,\dots,v_j)\right) \mathbb{P}\left((C_1 = v_1) \cap \dots \cap (C_j = v_j)\right).}$$

Q 31. Soit $j \in [\![1, n-1]\!]$. Prenons $(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j$. Alors $\dim(\mathrm{Vect}(v_1,\dots,v_j)) \leqslant j$, donc d'après la question 16, $\mathrm{card}(\mathrm{Vect}(v_1,\dots,v_j) \cap \mathcal{V}_{n,1}) \leqslant 2^j$. Puis, si $v \in \mathrm{Vect}(v_1,\dots,v_j) \cap \mathcal{V}_{n,1}$, d'après la question 25, $\mathbb{P}(C_{j+1} = v) = \dfrac{1}{2^n}$. Or $(C_{j+1} \in \mathrm{Vect}(v_1,\dots,v_j)) = (C_{j+1} \in \mathrm{Vect}(v_1,\dots,v_j) \cap \mathcal{V}_{n,1})$, donc

$$\mathbb{P}(C_{j+1} \in \mathrm{Vect}(v_1,\dots,v_j)) = \mathrm{card}(\mathrm{Vect}(v_1,\dots,v_j) \cap \mathcal{V}_{n,1}) \frac{1}{2^n} \leqslant 2^{j-n}.$$

D'après la question précédente,

$$\mathbb{P}(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)) \leqslant \sum_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j} 2^{j-n} \mathbb{P}\left((C_1 = v_1) \cap \dots \cap (C_j = v_j)\right) = 2^{j-n}$$

car $((C_1 = v_1) \cap \dots \cap (C_j = v_j))_{(v_1,\dots,v_j) \in \mathcal{V}_{n,1}^j}$ est un système complet d'évènements. On a donc bien $\boxed{\mathbb{P}(C_{j+1} \in \mathrm{Vect}(C_1,\dots,C_j)) \leqslant 2^{j-n}}$.

Q 32. D'après les questions 29 et 31,

$$\mathbb{P}(M_n \notin \mathcal{G}\ell_n(\mathbb{R})) \leqslant \sum_{j=1}^{n-1} 2^{j-n} = 2^{1-n} \frac{2^{n-1} - 1}{2 - 1} = 1 - \frac{1}{2^{n-1}}.$$

Ainsi, $\boxed{\mathbb{P}(M_n \in \mathcal{G}\ell_n(\mathbb{R})) = 1 - \mathbb{P}(\notin \mathcal{G}\ell_n(\mathbb{R})) \geqslant \dfrac{1}{2^{n-1}}}$.

III Un autre procédé de construction de matrices aléatoires à coefficients dans $\{-1, 1\}$

Q 33. Pas besoin de tester si le coefficient vaut 1, mais on le fait quand-même pour la lisibilité.

```
def modifie_matrice(p, A):
    n, m = A.shape
    for i in range(n):
        for j in range(m):
            if A[i,j] = 1 and rd.binomial(1, p) == 1:
                A[i,j] = -1
```

Q 34. Pour tester si $A_k = -A_0$, on peut calculer la somme des coefficients de A_k : on aura $A_k = -A_0$ ssi cette somme vaut $-n^2$.

```
def nb_tours(p, n):
    A = np.ones((n, n))
    k = 0
    while A.sum() > -n**2:
        modifie_matrice(p, A)
        k = k + 1
    return k
```

Q 35. Rien de particulier ici.

```
def moyenne_tours(p, n, nbe):
    s = 0
    for i in range(nbe):
        s = s + nb_tours(p, n)
    return s/nbe
```

IV Vecteurs aléatoires unitaires

Q 36. Notons $E = \left\{|\langle u_i|u_j\rangle|, (i,j) \in I^2, i \neq j\right\}$. Comme I a au moins deux éléments, E est non vide. Soit $(i,j) \in I^2$ avec $i \neq j$. Alors d'après l'inégalité de Cauchy-Schwarz : $|\langle u_i|u_j\rangle| \leqslant \langle u_i|u_i\rangle\langle u_j|u_j\rangle = 1$ car les vecteurs sont unitaires.
Ainsi, $\boxed{E \subset [0,1] \text{ : c'est une partie non vide majorée de } \mathbb{R}}$. E admet donc une borne supérieure. De plus, sa borne supérieure est dans $[0,1]$.

Q 37. Supposons que $C(u) = 0$. Alors pour tout $(i,j) \in I^2$ avec $i \neq j$, $|\langle u_i|u_j\rangle| \leqslant 0$, donc $\langle u_i|u_j\rangle = 0$ et u_i et u_j sont orthogonaux.
Ainsi, la famille u est une famille orthogonale, qui est donc libre : comme $\dim(\mathcal{M}_{n,1}(\mathbb{R})) = n$, u est une famille finie qui a au maximum n éléments. D'où $\boxed{\operatorname{card}\{u_i, i \in I\} \leqslant n}$.

Q 38. On peut prendre le logarithme de l'inégalité puis faire une étude de fonction, ou bien passer par les séries entières : les fonctions $t \mapsto \operatorname{ch}(t)$ et $t \mapsto \exp\left(\dfrac{t^2}{2}\right)$ sont développables en série entière sur $\mathbb{R}$ avec :

$$\forall t \in \mathbb{R}, \quad \operatorname{ch}(t) = \sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n)!} \quad \text{et} \quad \exp\left(\frac{t^2}{2}\right) = \sum_{n=0}^{+\infty} \frac{t^{2n}}{2^n n!}.$$

Or, pour $n = 0$, $\dfrac{1}{(2n)!} = \dfrac{1}{2^n n!}$ et pour $n \geqslant 1$,

$$\frac{2^n n!}{(2n)!} = \frac{1}{\prod_{k=1}^{n}(2k-1)} \leqslant 1 \quad \text{donc} \quad \frac{1}{(2n)!} \leqslant \frac{1}{2^n n!}.$$

D'où, $\boxed{\forall t \in \mathbb{R}, \operatorname{ch}(t) \leqslant \exp\left(\frac{t^2}{2}\right)}$.

Q 39. Soit $t \in \mathbb{R}$. Alors

$$\exp\left(t\langle X|Y\rangle\right) = \exp\left(\sum_{k=1}^{n} \frac{t}{n} X_k Y_k\right) = \prod_{k=1}^{n} \exp\left(\frac{t}{n} X_k Y_k\right).$$

Or, d'après le lemme des coalitions, les variables aléatoires $\exp\left(\frac{t}{n} X_1 Y_1\right)$ et $\prod_{k=2}^{n} \exp\left(\frac{t}{n} X_k Y_k\right)$ sont indépendantes donc :

$$\mathbb{E}\left(\exp\left(t\langle X|Y\rangle\right)\right) = \mathbb{E}\left(\exp\left(\frac{t}{n} X_1 Y_1\right)\right) \mathbb{E}\left(\prod_{k=2}^{n} \exp\left(\frac{t}{n} X_k Y_k\right)\right)$$

et par une récurrence immédiate :

$$\mathbb{E}\left(\exp\left(t\langle X|Y\rangle\right)\right) = \prod_{k=1}^{n} \mathbb{E}\left(\exp\left(\frac{t}{n} X_k Y_k\right)\right).$$

Puis, si $k \in [\![1, n]\!]$, la variable $Z_k = X_k Y_k$ suit la loi $\mathcal{R}$ d'après 19, donc

$$\mathbb{E}\left(\exp\left(\frac{t}{n} X_k Y_k\right)\right) = \frac{1}{2}\exp\left(\frac{t}{n}\right) + \frac{1}{2}\exp\left(-\frac{t}{n}\right) = \operatorname{ch}\left(\frac{t}{n}\right).$$

D'où $\boxed{\mathbb{E}\left(\exp\left(t\langle X|Y\rangle\right)\right) = \prod_{k=1}^{n} \operatorname{ch}\left(\frac{t}{n}\right) = \left(\operatorname{ch}\left(\frac{t}{n}\right)\right)^n}$.

Q 40. D'après la question 38, pour tout $t \in \mathbb{R}$, $\operatorname{ch}\left(\frac{t}{n}\right) \leqslant \exp\left(\frac{(t/n)^2}{2}\right)$. Comme les deux côtés de l'inégalité sont positifs, on obtient :

$$\forall t \in \mathbb{R}, \quad \left(\operatorname{ch}\left(\frac{t}{n}\right)\right)^n \leqslant \left(\exp\left(\frac{t^2}{2n^2}\right)\right)^n = \exp\left(\frac{t^2}{2n}\right).$$

En appliquant la question précédente :

$$\boxed{\forall t \in \mathbb{R}, \quad \mathbb{E}\left(\exp(t\langle X|Y\rangle)\right) \leqslant \exp\left(\frac{t^2}{2n}\right).}$$

Q 41. Soit $t \in \mathbb{R}^+$. Posons $T = \exp(tZ)$. Par hypothèse, T est positive et admet un espérance finie, donc d'après l'inégalité de Markov appliquée à T :

$$\mathbb{P}(T \geqslant \exp(\lambda t)) \leqslant \frac{\mathbb{E}(T)}{\exp(\lambda t)} \leqslant \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$$

par hypothèse. Si $t \neq 0$ alors $(T \geqslant \exp(\lambda t)) = (tZ \geqslant \lambda t) = (Z \geqslant \lambda)$, donc $\boxed{\mathbb{P}(Z \geqslant \lambda) \leqslant \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)}$.

Si $t = 0$, alors le terme $\exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$ vaut 1, donc l'inégalité est aussi vérifiée.

Q 42. Prenons $U = -Z$. Alors pour tout $t \in \mathbb{R}$, $\exp(tU) = \exp((-t)Z)$ admet une espérance finie et

$$\mathbb{E}\left(\exp(tU)\right) = \mathbb{E}\left(\exp((-t)Z)\right) \leqslant \exp\left(\frac{\sigma^2(-t)^2}{2}\right).$$

D'après la question 41 appliquée à la variable U, on a donc :

$$\forall t \in \mathbb{R}^+, \quad \mathbb{P}(U \geqslant \lambda) \leqslant \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right).$$

Puis,

$$\forall t \in \mathbb{R}^+, \quad \mathbb{P}(|Z| \geqslant \lambda) = \mathbb{P}(Z \geqslant \lambda) + \mathbb{P}(U \geqslant \lambda) \leqslant 2\exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right).$$

On cherche alors t de sorte que : $\dfrac{\sigma^2 t^2}{2} - \lambda t = -\dfrac{\lambda^2}{2\sigma^2}$ ou encore $0 = \dfrac{\sigma^2 t^2}{2} - \lambda t + \dfrac{\lambda^2}{2\sigma^2} = \left(\dfrac{\sigma t}{\sqrt{2}} - \dfrac{\lambda}{\sigma\sqrt{2}}\right)^2$.

On pose donc $t = \dfrac{\lambda}{\sigma^2} \in \mathbb{R}^+$ et on obtient :

$$\boxed{\mathbb{P}(|Z| \geqslant \lambda) \leqslant 2\exp\left(-\frac{\lambda^2}{2\sigma^2}\right).}$$

Q 43. On pose $Z = \langle X|Y\rangle$. C'est une variable aléatoire réelle et pour tout $t \in \mathbb{R}$, $\exp(tZ)$ est d'espérance finie (car elle ne prend qu'un nombre fini de valeurs) et d'après la question 40, en posant $\sigma = \dfrac{1}{\sqrt{n}}$, on a bien

$$\mathbb{E}(\exp(tZ)) \leqslant \exp\left(\frac{\sigma^2 t^2}{2}\right).$$

On prend alors $\varepsilon \in [0,1]$. Si $\varepsilon = 0$, l'inégalité demandée est évidente, sinon on applique la question 42 en prenant $\lambda = \varepsilon$:

$$\boxed{\mathbb{P}(|\langle X|Y\rangle| \geqslant \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2 n}{2}\right).}$$

Q 44. Par sous-additivité :

$$\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| \geqslant \varepsilon\right) \leqslant \sum_{1\leqslant i<j\leqslant N} \mathbb{P}\left(|\langle X^i|X^j\rangle| \geqslant \varepsilon\right).$$

D'après la question 43, pour tout $(i,j) \in [\![1,n]\!]^2$ avec $i \neq j$, comme $X_1^i, \dots, X_n^i, Y_1^j, \dots, Y_n^j$ sont mutuellement indépendantes et de même loi $\mathcal{R}$, on a

$$\mathbb{P}(|\langle X^i|X^j\rangle| \geqslant \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2 n}{2}\right).$$

Ainsi,

$$\begin{aligned}\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| \geqslant \varepsilon\right) \leqslant \sum_{1\leqslant i<j\leqslant N} 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) &= 2\exp\left(-\frac{\varepsilon^2 n}{2}\right)\sum_{j=2}^{N}\sum_{i=1}^{j-1} 1\\ &= 2\exp\left(-\frac{\varepsilon^2 n}{2}\right)\sum_{j=1}^{N-1} j\\ &= 2\exp\left(-\frac{\varepsilon^2 n}{2}\right)\frac{N(N-1)}{2}\end{aligned}$$

D'où

$$\boxed{\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| \geqslant \varepsilon\right) \leqslant N(N-1)\exp\left(-\frac{\varepsilon^2 n}{2}\right).}$$

Q 45. Comme $n \geqslant 4\dfrac{\ln N}{\varepsilon^2}$, $\dfrac{\varepsilon^2 n}{2} \geqslant 2\ln(N)$ et $-\dfrac{\varepsilon^2 n}{2} \leqslant -2\ln(N)$. Par croissance de l'exponentielle :

$$N(N-1)\exp\left(-\frac{\varepsilon^2 n}{2}\right) \leqslant N(N-1)\exp(-2\ln(N)) = \frac{N(N-1)}{N^2} < 1.$$

D'après la question précédente :

$$\boxed{\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| \geqslant \varepsilon\right) \leqslant N(N-1)\exp\left(-\frac{\varepsilon^2 n}{2}\right) < 1.}$$

Q 46. Soit $N \in \mathbb{N}$ tel que $N \leqslant \exp\left(\dfrac{\varepsilon^2 n}{4}\right)$. Alors $n \geqslant \dfrac{4\ln(N)}{\varepsilon^2}$. D'après la question précédente,

$$\mathbb{P}\left(\bigcap_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| < \varepsilon\right) > 0.$$

Ainsi, $\displaystyle\bigcap_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| < \varepsilon$ est non vide : il existe au moins un $\omega \in \displaystyle\bigcap_{1\leqslant i<j\leqslant N} |\langle X^i|X^j\rangle| < \varepsilon$. Posons $u_i = X^i(\omega)$ pour tout $1 \leqslant i \leqslant N$. Alors par définition, $\boxed{C(u) < \varepsilon}$.

• • • FIN • • •