

Solution * Matrices à coefficients unitaires

Partie A.

Résultats préliminaires

1. Quels que soient $1 \leq i, j \leq n$,

$$[AB]_{i,j} = \sum_{k=1}^n a_{i,k} b_{k,j} \quad \text{et} \quad [BA]_{i,j} = \sum_{\ell=1}^n b_{i,\ell} a_{\ell,j}.$$

On en déduit que

$$\text{tr}(AB) = \sum_{i=1}^n \sum_{k=1}^n a_{i,k} b_{k,i} = \sum_{k=1}^n \sum_{i=1}^n b_{k,i} a_{i,k} = \text{tr}(BA).$$

|| L'égalité $\text{tr}(AB) = \text{tr}(BA)$ est vraie aussi pour $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ et $B \in \mathfrak{M}_{p,n}(\mathbb{K})$.

2. Quelles que soient les matrices A et B de $\mathfrak{M}_n(\mathbb{K})$,

$$\text{tr}(A^T \cdot B) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} b_{i,j}.$$

En particulier,

$$\forall A \in \mathfrak{M}_n(\mathbb{R}), \quad \text{tr}(A^T \cdot A) = \sum_{i=1}^n \sum_{j=1}^n a_{i,j}^2$$

est une somme de carrés.

3. Si la matrice $A^T \cdot A$ est nulle, alors sa trace est nulle, donc

$$\|A\|^2 = \text{tr}(A^T \cdot A) = 0$$

et par conséquent la matrice A est nulle.

Propriétés de $\mathfrak{N}_n$

4. Si 0 n'était pas valeur propre, alors A serait inversible et par conséquent toutes les puissances de A seraient inversibles. Or A est nilpotente donc, à partir d'un certain rang, toutes les puissances de A sont nulles.

♣ La matrice A admet un polynôme annulateur de la forme X^d . Toutes les valeurs propres de A sont racines de ce polynôme annulateur, donc 0 est la seule valeur propre de A .

5. Comme la matrice A admet un polynôme annulateur scindé (de la forme X^d), elle est trigonalisable et par conséquent, sa trace (resp. son déterminant) est égale à la somme (resp. au produit) de ses valeurs propres comptées avec multiplicité.

D'après la question précédente, le spectre de A est égal à $\{0\}$, donc la trace et le déterminant sont nuls.

6. Si $M^d = 0_n$, alors $(M^2)^d = (M^d)^2 = 0_n$, donc M^2 est nilpotente.

7. Si $M^p = N^q = 0_n$, alors $M^r = N^r = 0_n$ pour tout entier r supérieur à p et à q . Comme M et N commutent, alors $(MN)^r = M^r N^r = 0_n$, donc MN est nilpotente.

♣ De même, comme M et N commutent, on déduit de la formule du binôme que

$$(M + N)^{2r} = \sum_{k=0}^{2r} \binom{2r}{k} M^k N^{2r-k}.$$

Pour $k \geq r$, on a $M^k = 0_n$ et donc $M^k N^{2r-k} = 0_n$; pour $0 \leq k < r$, on a $2r - k \geq r$, donc $N^{2r-k} = 0_n$ et aussi $M^k N^{2r-k} = 0_n$. Donc tous les termes du second membre sont nuls et $(M + N)^{2r} = 0_n$.

8. D'après [6.] et [7.], les matrices $(M + N)^2$, M^2 et N^2 sont nilpotentes. D'après [5.],

$$\text{tr}[(M + N)^2 - M^2 - N^2] = 0.$$

En développant,

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

|| *A priori, les matrices M et N ne commutent pas!*

D'après [1.], $\text{tr}(MN) = 0$.

9. Si $M \in \mathfrak{M}_2(\mathbb{R})$ est nilpotente, alors $\text{tr } M = \det M = 0$ d'après [5.].

Réciproquement, si $\text{tr } M = \det M = 0$, alors le polynôme caractéristique de $M \in \mathfrak{M}_2(\mathbb{R})$ est égal à

$$X^2 - (\text{tr } M)X + (\det M) = X^2$$

et d'après le théorème de Cayley-Hamilton, $M^2 = 0_2$, donc M est nilpotente.

10. Si M est symétrique réelle, alors elle est diagonalisable (Théorème spectral). D'après [5.], si M est nilpotente, alors sa seule valeur propre est 0. Donc M est semblable à la matrice nulle et donc égale à la matrice nulle.

11. La matrice $A^\top \cdot A$ est symétrique réelle.

Par ailleurs, comme A est antisymétrique, $A^\top \cdot A = -A^2$ et comme A est supposée nilpotente, alors $A^\top \cdot A$ est nilpotente [6.].

D'après la question précédente, la matrice $A^\top \cdot A$ est nulle et d'après [3.], la matrice A est nulle.

12. Si $n \geq 3$, alors $M = \text{Diag}(1, -1, 0, \dots, 0)$ est une matrice non nulle, dont le déterminant et la trace sont nuls. Comme $\text{Sp}(M) = \{-1; 0; 1\} \neq \{0\}$, on déduit de [4.] que M n'est pas nilpotente.

Partie B. Matrices aléatoires

Résultats algébriques

13. Comme $\mathcal{V}_{n,1} \subset \mathfrak{M}_{n,1}(\mathbb{R})$, le sous-espace engendré par $\mathcal{V}_{n,1}$ est un sous-espace de $\mathfrak{M}_{n,1}(\mathbb{R})$.

Réciproquement, il est clair que

$$\forall 1 \leq i \leq n, \quad E_i = \frac{1}{2}V - \frac{1}{2}(V - 2E_i)$$

et comme les colonnes V et $V - 2E_i$ appartiennent évidemment à $\mathcal{V}_{n,1}$, le sous-espace $\mathfrak{M}_{n,1}(\mathbb{R})$, engendré par les colonnes $E_1, \dots, E_n$, est contenu dans le sous-espace engendré par $\mathcal{V}_{n,1}$.

Par double inclusion,

$$\text{Vect}(\mathcal{V}_{n,1}) = \mathfrak{M}_{n,1}(\mathbb{R}).$$

14. Si $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$, alors la famille $(C_1, \dots, C_j, C_{j+1})$ est liée. Si la famille $(C_1, \dots, C_j)$ est libre, alors les familles $(C_1, \dots, C_k)$ sont libres pour tout entier $1 \leq k \leq j$. Il apparaît que l'entier j cherché est le plus grand élément de l'ensemble

$$\mathcal{L} = \{j \in \llbracket 1, n \rrbracket : \text{la famille } (C_1, \dots, C_j) \text{ est libre}\}.$$

Il existe donc *au plus un* tel entier j .

• Réciproquement, l'ensemble $\mathcal{L}$ est, par construction, une partie de $\mathbb{N}$ majorée par n . Comme $C_1 \neq 0$, la famille (C_1) est libre, donc $1 \in \mathcal{L}$. En tant que partie non vide et majorée de $\mathbb{N}$, l'ensemble $\mathcal{L}$ admet un plus grand élément j_0 .

Comme la famille $(C_1, \dots, C_n)$ est liée, l'entier n n'appartient pas à $\mathcal{L}$, donc $j_0 \leq n-1$ et $j_0 + 1 \leq n$. Par conséquent, comme $j_0 \in \mathcal{L}$, la famille $(C_1, \dots, C_{j_0})$ est libre et comme $j_0 + 1 \notin \mathcal{L}$ et $j_0 + 1 \leq n$, la famille $(C_1, \dots, C_{j_0}, C_{j_0+1})$ est liée.

15. Comme les colonnes $U_1, \dots, U_d$ sont linéairement indépendantes, l'espace $H = \text{Vect}(U_1, \dots, U_d)$ est un espace vectoriel de dimension d et le rang de la matrice

$$U = (u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq d}$$

est égal à d .

Le rang d'une matrice est aussi le rang de la famille des lignes. Par conséquent, on peut extraire de la famille $(L_1, \dots, L_n)$ une sous-famille libre de cardinal d : $(L_{i_1}, \dots, L_{i_d})$ avec $1 \leq i_1 < i_2 < \dots < i_d \leq n$. Le rang de la matrice

$$U_0 = (u_{i_k,j})_{1 \leq k,j \leq d} \in \mathfrak{M}_d(\mathbb{R})$$

est donc égal à d et cette matrice est inversible puisqu'elle est carrée (Théorème du rang).

Ces indices $i_1, \dots, i_d$ étant choisis, l'application $\Phi : H \rightarrow \mathfrak{M}_{d,1}(\mathbb{R})$ définie par l'énoncé est clairement une application linéaire.

Par définition des indices $i_1, \dots, i_d$, l'image par Φ de la famille $(U_1, \dots, U_d)$ est la famille des colonnes de la matrice U_0 . Comme cette matrice U_0 est inversible, l'image d'une base de H par Φ est donc une base de $\mathfrak{M}_{d,1}(\mathbb{R})$, donc Φ est un isomorphisme et en particulier une bijection de H sur $\mathfrak{M}_{d,1}(\mathbb{R})$.

16. Si $\mathcal{W}$ est un sous-espace vectoriel de dimension d de $\mathfrak{M}_{n,1}(\mathbb{R})$, alors il existe une base de $\mathcal{W}$ de la forme $(U_1, \dots, U_d)$ et l'application Φ définie à la question précédente réalise une bijection de $\mathcal{W}$ sur $\mathfrak{M}_{d,1}(\mathbb{R})$.

En particulier, l'image par Φ d'un vecteur de $\mathcal{W} \cap \mathcal{V}_{n,1}$ est un vecteur de $\mathcal{V}_{d,1}$ et comme Φ est injective,

$$\#(\mathcal{W} \cap \mathcal{V}_{n,1}) \leq \#(\mathcal{V}_{d,1}) = 2^d.$$

Loi de Rademacher

17. Si $X(\omega) = 1$ (resp. -1), alors $(X(\omega) + 1)/2 = 1$ (resp. 0). Donc

$$[Y = 0] = [X = -1], \quad [Y = 1] = [X = 1]$$

et la variable aléatoire $Y = (X + 1)/2$ est une variable aléatoire de Bernoulli, de paramètre

$$P(Y = 1) = P(X = 1) = 1/2.$$

18. On sait que $E(Y) = p = 1/2$ et $V(Y) = pq = 1/4$. Par linéarité de l'espérance, $E(X) = 2E(Y) - 1 = 0$ et par propriété de la variance,

$$V(X) = 2^2 V(Y) = 1.$$

|| On peut aussi remarquer que $V(Y) = E(Y^2) = 1$ puisque Y est centrée et que Y^2 est constamment égale à 1.

19. Comme au [17.], on commence par déterminer les valeurs prises par la variable aléatoire $Z = XY$. On constate facilement que

$$[Z = 1] = [X = 1, Y = 1] \sqcup [X = -1, Y = -1] \quad \text{et que} \quad [Z = -1] = [X = 1, Y = -1] \sqcup [X = -1, Y = 1].$$

On en déduit que $P(Z = 1) = P(Z = -1) = 1/2$ avec l'indépendance de X et Y . Autrement dit, le produit XY suit encore la loi de Rademacher.

Procédé de génération

20. La variable aléatoire τ_n est une somme de n variables aléatoires indépendantes et de même loi. Chacune de ces variables est bornée, donc admet un moment d'ordre deux. Donc τ_n est une variable d'espérance finie et de variance finie, avec $E(\tau_n) = n E(m_{1,1}) = 0$ et $V(\tau_n) = n V(m_{1,1}) = n$.

21. La formule développée du déterminant

$$\delta_n = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) m_{1,\sigma(1)} \cdots m_{n,\sigma(n)} \quad (*)$$

prouve que δ_n est une variable aléatoire bornée (puisque les $m_{i,j}$ sont toutes bornées). Par conséquent, δ_n est une variable aléatoire d'espérance finie et de variance finie.

♣ Par linéarité de l'espérance,

$$E(\delta_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) E(m_{1,\sigma(1)} \cdots m_{n,\sigma(n)}).$$

Les variables aléatoires $m_{i,\sigma(i)}$ sont indépendantes et d'espérance finie (elles sont bornées), donc

$$\forall \sigma \in \mathfrak{S}_n, \quad E(m_{1,\sigma(1)} \cdots m_{n,\sigma(n)}) = \prod_{i=1}^n E(m_{i,\sigma(i)}) = 0$$

puisque les $m_{i,j}$ sont centrées. Ainsi $E(\delta_n) = 0$.

22. Comme δ_n est centrée, sa variance est en fait égale à $E(\delta_n^2)$ (formule de Koenig-Huyghens). On s'arme de courage et on se lance dans les calculs! Par linéarité de l'espérance une fois encore,

$$\begin{aligned} E(\delta_n^2) &= E\left(\sum_{\sigma \in \mathfrak{S}_n} \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\sigma)\varepsilon(\tau) m_{1,\sigma(1)} \cdots m_{n,\sigma(n)} \cdot m_{1,\tau(1)} \cdots m_{n,\tau(n)}\right) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\sigma)\varepsilon(\tau) E(m_{1,\sigma(1)} \cdots m_{n,\sigma(n)} \cdot m_{1,\tau(1)} \cdots m_{n,\tau(n)}). \end{aligned}$$

Pour $\sigma \neq \tau$, il existe au moins un indice i tel que $\sigma(i) \neq \tau(i)$. Dans ces conditions, la variable aléatoire $m_{i,\sigma(i)}$ (qui est centrée, on l'a déjà remarqué) n'apparaît qu'une seule fois dans le produit

$$m_{1,\sigma(1)} \cdots m_{n,\sigma(n)} \cdot m_{1,\tau(1)} \cdots m_{n,\tau(n)}$$

et on déduit du lemme des coalitions que l'espérance de ce produit est nulle.

Dans l'expression développée (*) du déterminant, chaque terme suit une loi de Rademacher (en tant que produit de variables de Rademacher indépendantes, cf [19.]) mais il n'est pas possible d'appliquer le lemme des coalitions : pour une permutation σ qui admet 1 pour point fixe (et il y en a $(n-1)!$, dont l'identité), les variables

$$m_{1,\sigma(1)} \cdots m_{n,\sigma(n)} = m_{1,1} m_{2,\sigma(2)} \cdots m_{n,\sigma(n)} \quad \text{et} \quad m_{1,1} m_{2,2} \cdots m_{n,n}$$

ne sont a priori pas indépendantes.

Le raisonnement précédent a permis de prouver que les termes de cette combinaison linéaire sont deux à deux décorrélés et cela suffit pour calculer facilement la variance.

Il ne reste donc que les termes pour lesquels $\sigma = \tau$:

$$\mathbf{E}(\delta_n^2) = \sum_{\sigma \in \mathfrak{S}_n} [\varepsilon(\sigma)]^2 \mathbf{E}((m_{1,\sigma(1)} \cdots m_{n,\sigma(n)})^2) = \sum_{\sigma \in \mathfrak{S}_n} 1 = n!$$

puisque $[\varepsilon(\sigma)]^2 = (\pm 1)^2 = 1$ et que $m_{i,j}^2(\omega) = 1$ pour tout $\omega \in \Omega$.

On a bien $\mathbf{V}(\delta_n) = n!$.

23. D'après [9.], la matrice M_2 est nilpotente si, et seulement si, $\det(M_2) = \text{tr}(M_2) = 0$, c'est-à-dire

$$m_{1,1} + m_{2,2} = m_{1,1}m_{2,2} - m_{1,2}m_{2,1} = 0.$$

Comme les $m_{i,j}$ sont égaux à ± 1 , ils sont égaux à leurs inverses, donc

$$m_{1,1} + m_{2,2} = 0 \iff m_{1,1}m_{2,2} = -1$$

et par conséquent,

$$\begin{cases} m_{1,1} + m_{2,2} = 0 \\ m_{1,1}m_{2,2} - m_{1,2}m_{2,1} = 0 \end{cases} \iff \begin{cases} m_{1,1}m_{2,2} = -1 \\ m_{1,2}m_{2,1} = -1. \end{cases}$$

Autrement dit,

$$[M_2 \in \mathcal{N}_2] = [m_{1,1}m_{2,2} = -1] \cap [m_{1,2}m_{2,1} = -1] \in \mathcal{A}.$$

Les indices restant bien séparés, on peut appliquer le lemme des coalitions : les variables aléatoires $m_{1,1}m_{2,2}$ et $m_{1,2}m_{2,1}$ sont indépendantes.

D'après [19.], ces deux variables aléatoires suivent la loi de Rademacher (produit de deux variables aléatoires de Rademacher indépendantes). Par conséquent,

$$\mathbf{P}(M_2 \in \mathcal{N}_2) = \mathbf{P}(m_{1,1}m_{2,2} = -1) \mathbf{P}(m_{1,2}m_{2,1} = -1) = \mathbf{P}(m_{1,1} = -1) \mathbf{P}(m_{1,1} = -1) = 1/4.$$

|| *Toute variable aléatoire qui suit la loi de Rademacher a, de fait, même loi que $m_{1,1}$, ce qui permet d'alléger les notations pour finir le calcul.*

24. Comme on l'a observé à la question précédente,

$$[M_2 \in \text{GL}_2(\mathbb{R})] = [m_{1,1}m_{2,2} - m_{1,2}m_{2,1} = 0] \in \mathcal{A}$$

et d'autre part les variables aléatoires $m_{1,1}m_{2,2}$ et $m_{2,1}m_{1,2}$ sont indépendantes et suivent la loi de Rademacher. Donc le couple $(m_{1,1}m_{2,2}; m_{2,1}m_{1,2})$ a même loi que le couple $(m_{1,1}; m_{2,2})$. Par conséquent,

$$\begin{aligned} \mathbf{P}(M_2 \in \text{GL}_2(\mathbb{R})) &= \mathbf{P}(m_{1,1} = m_{2,2}) = \mathbf{P}(m_{1,1} = 1, m_{2,2} = 1) + \mathbf{P}(m_{1,1} = -1, m_{2,2} = -1) \\ &= 2[\mathbf{P}(m_{1,1} = 1)]^2 = 1/2 \end{aligned} \quad (*)$$

où (*) on a décomposé l'évènement $[m_{1,1} = m_{2,2}]$ sur le système complet d'évènements associé à $m_{1,1}$ (selon la méthode traditionnelle).

Généralisation

26. Les coefficients de la colonne $C(\omega)$ sont égaux à ± 1 , donc la colonne $C(\omega)$ n'est pas nulle. Par conséquent, si le couple $(C(\omega), C'(\omega))$ est une famille liée, alors il existe un scalaire $\alpha \in \mathbb{R}$ tel que $C'(\omega) = \alpha C(\omega)$.

27. D'après [26.], la probabilité pour que le couple (C, C') soit une famille liée est égale à

$$\mathbf{P}(C = \pm C') = \mathbf{P}(C = C') + \mathbf{P}(C = -C').$$

Comme on l'a observé plus haut [23.], les coefficients des deux colonnes sont égaux à ± 1 . Par conséquent,

$$[c_1 = c'_1, \dots, c_n = c'_n] = [c_1c'_1 = 1, \dots, c_nc'_n = 1] \quad \text{et} \quad [c_1 = -c'_1, \dots, c_n = -c'_n] = [c_1c'_1 = -1, \dots, c_nc'_n = -1].$$

On a également déjà remarqué que les variables aléatoires $c_1c'_1, \dots, c_nc'_n$ étaient indépendantes (lemme des coalitions) et suivaient toutes la loi de Rademacher (en tant que produits de deux variables aléatoires de Rademacher indépendantes [19.]). Donc

$$(c_1c'_1, \dots, c_nc'_n) \stackrel{d}{=} (c_1, \dots, c_n)$$

et par conséquent,

$$\begin{aligned} \mathbf{P}(C = \pm C') &= \mathbf{P}(c_1 = 1, c_2 = 1, \dots, c_n = 1) + \mathbf{P}(c_1 = -1, c_2 = -1, \dots, c_n = -1) \\ &= 2 \cdot 2^{-n} = 2^{1-n} \end{aligned}$$

d'après [25.].

28. Toute fonction d'un vecteur aléatoire discret est une variable aléatoire discrète. Par exemple, $\text{rg}(C_1, \dots, C_j)$ est une variable aléatoire discrète et en particulier $[\text{rg}(C_1, \dots, C_j) = j]$ est un évènement (qui signifie que la famille $(C_1, \dots, C_j)$ est libre).

Les variables aléatoires $C_1, \dots, C_j, C_{j+1}$ prennent leurs valeurs dans $\mathcal{V}_{n,1}$, donc

$$[C_{j+1} \in \text{Vect}(C_1, \dots, C_j)] = \bigsqcup_{(v_1, \dots, v_j) \in \mathcal{V}_{n,1}^j} [C_1 = v_1, \dots, C_j = v_j, C_{j+1} \in \text{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}].$$

Comme $C_1, \dots, C_{j+1}$ sont des variables aléatoires discrètes et que l'ensemble $\mathcal{V}_{n,1}^j$ est fini [16.], le second membre de cette égalité appartient bien à la tribu $\mathcal{A}$.

On a ainsi démontré que $R_1, \dots, R_{n-1}$ et R_n étaient bien des évènements.

|| *Il est probable qu'on n'attendait pas une telle justification.*

✱ Comme $R_1, \dots, R_n$ sont des évènements, la famille $(R_1, \dots, R_n)$ est un système complet d'évènements si, et seulement si, c'est une partition de Ω , c'est-à-dire si chaque $\omega \in \Omega$ appartient à un, et un seul, des évènements R_j .

Soit $\omega \in \Omega$.

Si la famille $(C_1(\omega), \dots, C_n(\omega))$ est libre, alors $\omega \in R_n$ (par définition de R_n).

Si, au contraire, cette famille est liée, alors [14.] il existe un, et un seul, entier $1 \leq j \leq n-1$ tel que $\omega \in R_j$.

On a ainsi démontré que

$$\Omega = \bigsqcup_{k=1}^n R_k$$

et donc que $(R_k)_{1 \leq k \leq n}$ est bien un système complet d'évènements.

29. La matrice M est singulière (= non inversible) si, et seulement si, ses colonnes $C_1, \dots, C_n$ forment une famille liée. Autrement dit, d'après [28.],

$$[M \notin \text{GL}_n(\mathbb{R})] = \bigsqcup_{k=1}^{n-1} R_k$$

et donc, par additivité de $\mathbf{P}$,

$$\mathbf{P}(M \notin \text{GL}_n(\mathbb{R})) = \sum_{k=1}^{n-1} \mathbf{P}(R_k).$$

Par définition, $R_k \subset [C_{j+1} \in \text{Vect}(C_1, \dots, C_j)]$ et par croissance de $\mathbf{P}$,

$$\mathbf{P}(M \notin \text{GL}_n(\mathbb{R})) \leq \sum_{k=1}^{n-1} \mathbf{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j)).$$

30. On décompose l'évènement $[C_{j+1} \in \text{Vect}(C_1, \dots, C_j)]$ dans le système complet d'évènements associé au vecteur aléatoire $(C_1, \dots, C_j)$:

$$\begin{aligned} \mathbf{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j)) &= \sum_{(v_1, \dots, v_j) \in \mathcal{V}_{n,1}^j} \mathbf{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j), C_1 = v_1, \dots, C_j = v_j) \\ &= \sum_{(v_1, \dots, v_j) \in \mathcal{V}_{n,1}^j} \mathbf{P}(C_{j+1} \in \text{Vect}(v_1, \dots, v_j)) \mathbf{P}(C_1 = v_1, \dots, C_j = v_j) \end{aligned}$$

car d'une part

$$\begin{aligned} [C_{j+1} \in \text{Vect}(C_1, \dots, C_j), C_1 = v_1, \dots, C_j = v_j] &= [C_{j+1} \in \text{Vect}(v_1, \dots, v_j), C_1 = v_1, \dots, C_j = v_j] \\ &= [C_{j+1} \in \text{Vect}(v_1, \dots, v_j)] \cap [C_1 = v_1, \dots, C_j = v_j] \end{aligned}$$

et d'autre part la variable aléatoire C_{j+1} et le vecteur aléatoire $(C_1, \dots, C_j)$ sont indépendants (lemme des coalitions).

31. La somme précédente compte $(2^n)^j = 2^{nj}$ termes.

Comme on l'a déjà remarqué [28.],

$$[C_{j+1} \in \text{Vect}(v_1, \dots, v_j)] = [C_{j+1} \in \text{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}].$$

D'après [16.], le cardinal de $\text{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}$ est inférieur à 2^j et par [25.]

$$\forall (\varepsilon_1, \dots, \varepsilon_n) \in \text{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}, \quad \mathbf{P}(C_{j+1} = (\varepsilon_1, \dots, \varepsilon_n)) = 2^{-n},$$

donc

$$\mathbf{P}(C_{j+1} \in \text{Vect}(v_1, \dots, v_j)) \leq 2^j \cdot 2^{-n}.$$

Enfin, comme les variables aléatoires $C_1, \dots, C_j$ sont indépendantes, on déduit de [25.] que

$$\mathbf{P}(C_1 = v_1, \dots, C_j = v_j) = \mathbf{P}(C_1 = v_1) \cdots \mathbf{P}(C_j = v_j) = (2^{-n})^j.$$

Par conséquent,

$$\begin{aligned} \mathbf{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j)) &= \sum_{(v_1, \dots, v_j) \in \mathcal{V}_{n,1}^j} \mathbf{P}(C_{j+1} \in \text{Vect}(v_1, \dots, v_j)) \mathbf{P}(C_1 = v_1, \dots, C_j = v_j) \\ &\leq 2^{nj} \cdot 2^{j-n} \cdot 2^{-nj} = 2^{j-n}. \end{aligned}$$

32. D'après [29.] et [31.],

$$\mathbf{P}(M \notin \text{GL}_n(\mathbb{R})) \leq \sum_{j=1}^{n-1} 2^{j-n} = 2^{-n} \cdot 2 \cdot \frac{2^{n-1} - 1}{2 - 1} = 1 - 2^{1-n}$$

et par passage au complémentaire

$$\mathbf{P}(M \in \text{GL}_n(\mathbb{R})) \geq \frac{1}{2^{n-1}}.$$

|| Pour $n = 2$, on a trouvé $\mathbf{P}(M \in \text{GL}_2(\mathbb{R})) = 1/2$ et la minoration qu'on vient de trouver est optimale en ce sens.

Partie C. Autre procédé de génération

33. Il est préférable de se servir des rappels fournis par l'énoncé (qui sont en fait des indications).

Ainsi, au lieu de supposer que l'argument A est une matrice carrée et de récupérer le nombre de lignes de cette matrice avec `len(A)`, il vaut mieux récupérer le nombre de lignes et le nombre de colonne avec `n, p = A.shape`.

✱ En ce qui concerne les entrées/sorties, il est capital de suivre les spécifications imposées par l'énoncé. Cette première fonction modifie le contenu du tableau A passé en argument, mais ne renvoie rien. C'est donc une faute grave de terminer cette fonction par une instruction `return` (quelle que soit la valeur renvoyée).

34. Si A et B sont deux tableaux numpy (de même format), alors la comparaison $A==B$ renvoie un tableau de booléens (de même format que A et B). Cette comparaison ne peut donc pas être utilisée dans une boucle `while`.

Le mieux est une fois de plus de suivre l'énoncé : si A est une matrice dont tous les coefficients sont égaux à ± 1 , alors les coefficients de A sont tous égaux à -1 si, et seulement si, la somme de ses coefficients `A.sum()` est égale à $-n^2$.

35. Sans difficulté particulière, à savoir faire sans hésitation.

Partie D. Vecteurs aléatoires unitaires

36. Comme les vecteurs u_i sont supposés unitaires, on déduit de l'inégalité de Schwarz que $0 \leq |\langle u_i | u_j \rangle| \leq \|u_i\| \|u_j\| = 1$. Comme il y a au moins deux indices dans I , on considère ici une partie non vide du segment $[0, 1]$ et on déduit de l'axiome de la borne supérieure que cette partie admet une borne supérieure réelle, comprise entre 0 et 1.

37. Si $C(u) = 0$, alors les vecteurs u_i sont deux à deux orthogonaux. Ainsi, la famille $(u_i)_{i \in I}$ est une famille orthonormée et donc libre. En particulier, le cardinal de I est inférieur à la dimension de l'espace : $\#(I) \leq n$.

|| Une famille orthogonale de vecteurs **non nuls** est une famille libre. Une famille orthogonale qui contient le vecteur nul est nécessairement une famille liée.

38. Il suffit de comparer les coefficients des deux séries entières. (Très, très classique dans ce contexte.)

39. Par définition du produit scalaire,

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

Comme $X_k Y_k$ suit la loi de Rademacher [19.], la variable aléatoire $\exp[(t/n) X_k Y_k]$ est une variable aléatoire d'espérance finie (elle est bornée!) et on déduit de la formule de transfert que

$$\mathbf{E}(\exp[(t/n) X_k Y_k]) = \text{ch} \frac{t}{n}.$$

On a ici affaire à un produit de variables aléatoires indépendantes (toujours le lemme des coalitions), de même loi et d'espérance finie, donc

$$\mathbf{E}[\exp(t \langle X | Y \rangle)] = \left(\text{ch} \frac{t}{n}\right)^n.$$

40. On majore l'expression trouvée à l'aide de l'inégalité du [38.]. Bien entendu, il faut préciser que les deux membres de l'inégalité [38.] sont positifs pour justifier l'élévation à la puissance n . (Inutile d'entrer dans les détails.)

41. Si $t > 0$, alors la fonction $[x \mapsto \exp(tx)]$ est *strictement* croissante et par conséquent,

$$\forall \omega \in \Omega, \quad Z(\omega) \geq \lambda \iff \exp(tZ(\omega)) \geq \exp(t\lambda)$$

c'est-à-dire

$$[Z \geq \lambda] = [\exp(tZ) \geq \exp(t\lambda)].$$

Comme $e^{t\lambda} > 0$ et que $\exp(tZ)$ est une variable aléatoire positive d'espérance finie, on peut appliquer l'inégalité de Markov.

• Le cas $t = 0$ est un cas particulier sans aucun intérêt mathématique. Il a un intérêt (purement) pédagogique cependant! En effet, pour $t = 0$, on a

$$[Z \geq \lambda] \subset \Omega = [1 \geq 1] = [\exp(tZ) \geq \exp(t\lambda)]$$

et la comparaison qu'on déduit de l'inégalité de Markov est encore vraie (quoique totalement dénuée d'intérêt).

Ce détail a pour objectif d'attirer l'attention sur les fonctions monotones.

Si la fonction f est strictement croissante, alors

$$[Z \geq \lambda] = [f(Z) \geq f(\lambda)]$$

mais si la fonction f est seulement croissante (au sens large), alors

$$[Z \geq \lambda] \subset [f(Z) \geq f(\lambda)].$$

C'est sur les évènements qu'il faut raisonner en premier lieu, pas sur les probabilités!

42. Il faut remarquer dans un premier temps que, dans le résultat précédent, le membre de gauche est indépendant du paramètre $t \in \mathbb{R}_+$. Autrement dit : le membre de gauche $\mathbf{P}(Z \geq \lambda)$ est un **minorant** de la fonction de t et il est donc majoré par la borne inférieure de la fonction.

|| La borne inférieure est le plus grand des minorants.

• Dans un second temps, il faut remarquer que la variable aléatoire $-Z$ vérifie les mêmes hypothèses de Z (puisque $tZ = (-t)(-Z)$ et que le majorant de l'espérance est une fonction paire de t). On peut alors déduire de l'égalité (entre évènements)

$$[Z \leq -\lambda] = [-Z \geq \lambda]$$

que

$$\forall t \in \mathbb{R}_+, \quad \mathbf{P}(Z \leq -\lambda) \leq \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right).$$

• Enfin, comme $\lambda > 0$,

$$[|Z| \geq \lambda] = [Z \geq \lambda] \cup [Z \leq -\lambda]$$

et on conclut par additivité de $\mathbf{P}$.

43. Si $\varepsilon > 0$, alors on choisit $\lambda = \varepsilon$ et $\sigma = 1/\sqrt{n}$, ce qui permet de conclure avec la question précédente.

• Si $\varepsilon = 0$ (cas particulier à nouveau dénué d'intérêt mathématique), l'évènement $[|X| \geq \varepsilon]$ est évidemment certain et le majorant est égal à 2 : la majoration est donc encore vraie...

|| La majoration n'a d'intérêt que si $\varepsilon^2 n \geq 2 \ln 2$!

44. Par sous-additivité de $\mathbf{P}$, quels que soient les évènements $(A_{i,j})_{1 \leq i < j \leq N}$,

$$\mathbf{P}\left(\bigcup_{1 \leq i < j \leq N} A_{i,j}\right) \leq \sum_{1 \leq i < j \leq N} \mathbf{P}(A_{i,j}).$$

On majore chaque terme avec le résultat de la question précédente et il reste à déterminer le nombre de termes de cette somme. C'est tout simple : chaque terme correspond au choix d'une paire $\{i, j\}$ d'éléments (distincts!) parmi $[1, N]$, il y a donc $\binom{N}{2} = \frac{N(N-1)}{2}$ termes dans la somme.

45. Par hypothèse, $n\varepsilon^2/2 \geq 2 \ln N$, donc le majorant obtenu à la question précédente est inférieur à $N(N-1)/N^2$ et donc strictement inférieur à 1.

46. En passant au complémentaire, on obtient un évènement de probabilité strictement positive et donc non vide!

• Évidemment, le résultat obtenu n'est intéressant que si $N \geq 2$!

Ayant choisi $\varepsilon > 0$, tant que la dimension n est assez petite pour que $\exp(n\varepsilon^2/4) < 2$, la méthode probabiliste ne donne rien d'intéressant : on sait [37.] que, pour tout $N \leq n$, il existe une famille de N vecteurs unitaires dont le paramètre de cohérence est nul!

En revanche, lorsque la dimension n grandit, la valeur de N peut devenir très grande devant la dimension n et on sait ainsi qu'il existe des familles "presque orthogonales" de cardinal très supérieur à la dimension de l'espace.