MATHÉMATIQUES APPROFONDIES - Maths I HEC-ESSEC 2024
Proposition de corrigé par David Meneu

Partie I : existence des matrices de Hadamard

Soit $n \geqslant 2$. On suppose dans toute cette partie I qu'il existe une matrice de Hadamard $H \in \mathcal{M}_n(\mathbb{R})$. On note $c_1, \ldots, c_n \in \mathcal{M}_{n,1}(\mathbb{R})$ ses vecteurs colonnes et $\ell_1, \ldots, \ell_n \in \mathcal{M}_{1,n}(\mathbb{R})$ ses vecteurs lignes.

1. Soit $P \in \mathcal{M}_n(\mathbb{R})$ une matrice de permutation, et σ la bijection de $[\![1\,;n]\!]$ dans lui-même associée. Alors, pour tout $(i,j) \in [\![1\,;n]\!]^2$:

$$^{\mathrm{t}}c_i \times c_j = \sum_{k=1}^{n} P_{i,k}P_{j,k} = \sum_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{j,\sigma(k)}$$

Si $i \neq j$, alors le produit des deux symboles de Kronecker est toujours nul car il est impossible que $\sigma(k)$, pour n'importe quel entier $k \in [\![1\,;n]\!]$, soit égal à la fois à i et à j.

Si par contre $i = j$, alors $^{\mathrm{t}}c_i \times c_i = \sum_{k=1}^{n} \delta_{i,\sigma(k)}^2 = 1$ car il existe, par bijectivité de σ, un unique entier $k \in [\![1\,;n]\!]$ tel que $i = \sigma(k)$ (un et un seul terme de la somme est non nul, et égal à 1).

Les colonnes de P forment donc une famille orthonormée de $\mathcal{M}_{n,1}(\mathbb{R})$ pour le produit scalaire canonique sur cet espace : P est bien une matrice orthogonale.

La matrice $^{\mathrm{t}}P$ (qui est de fait, aussi égale à P^{-1}) a pour coefficients :

$$P_{j,i} = \delta_{j,\sigma(i)} = \begin{cases} 1 & \text{si } \sigma(i) = j \iff i = \sigma^{-1}(j) \\ 0 & \text{sinon} \end{cases} = \delta_{i,\sigma^{-1}(j)}.$$

La matrice $^{\mathrm{t}}P$ est donc aussi une matrice de permutation, associée à la permutation σ^{-1}.

2. Soit $Q \in \mathcal{M}_n(\mathbb{R})$. Pour tout $(i,j) \in [\![1\,;n]\!]^2$: $(^{\mathrm{t}}QQ)_{i,j} = \sum_{k=1}^{n} Q_{k,i}Q_{k,j}$ correspond au produit scalaire des colonnes c_i et c_j de Q.

Le fait que les vecteurs colonnes de Q soient deux à deux orthogonaux est donc équivalent au fait que $^{\mathrm{t}}QQ$ soit une matrice diagonale.

Le fait que $Q_{i,j}^2 = 1$ pour tout $(i,j) \in [\![1\,;n]\!]^2$, est équivalent au fait que $Q_{i,j} \in \{-1\,;1\}$, qui a pour conséquence si $i = j$, que $(^{\mathrm{t}}QQ)_{i,i} = \sum_{k=1}^{n} Q_{k,i}^2 = n$ comme somme de carrés de n termes qui appartiennent tous à $\{-1\,;1\}$, et in fine que la matrice $^{\mathrm{t}}QQ$ est donc une matrice diagonale dont les coefficients diagonaux sont tous égaux à n : $^{\mathrm{t}}QQ = nI_n$.

D'où l'équivalence :

$$Q \text{ est une matrice de Hadamard} \iff {}^{\mathrm{t}}QQ = nI_n \quad \text{et } \forall (i,j) \in [\![1\,;n]\!]^2,\ Q_{i,j}^2 = 1.$$

3. D'après le critère précédent, H étant une matrice de Hadamard : $^{\mathrm{t}}HH = nI_n$ donc H est inversible, d'inverse $\frac{1}{n}\,{}^{\mathrm{t}}H$, de sorte que $^{\mathrm{t}}(^{\mathrm{t}}H)\,{}^{\mathrm{t}}H = H\,{}^{\mathrm{t}}H = nI_n$, et pour tout $(i,j) \in [\![1\,;n]\!]^2$, $(^{\mathrm{t}}H)_{i,j}^2 = H_{j,i}^2 = 1$, ce qui prouve que $^{\mathrm{t}}H$ est une matrice de Hadamard.

4. Soit $D \in \mathcal{M}_n(\mathbb{R})$ une matrice diagonale ne comportant que les valeurs -1 et 1 sur sa diagonale, et $P \in \mathcal{M}_n(\mathbb{R})$ une matrice de permutation.

D'après **1.**, P est alors orthogonale et ${}^{\mathrm{t}}P$ est aussi une matrice de permutation. Soit σ la permutation de $[\![1\,;n]\!]$ associée à P : pour tout $(i,k) \in [\![1\,;k]\!]^2$, $P_{i,k} = \delta_{i,\sigma(k)} = \begin{cases} 1 \text{ si } i = \sigma(k) \iff k = \sigma^{-1}(i) \\ 0 \text{ sinon} \end{cases}$.

- Pour tout $(i,j) \in [\![1\,;n]\!]^2$:

$$(PH)_{i,j}^2 = \Big(\sum_{k=1}^{n} P_{i,k}H_{k,j}\Big)^2 = H_{\sigma^{-1}(i),j}^2 = 1,$$

et : ${}^{\mathrm{t}}(PH)PH = {}^{\mathrm{t}}H\,{}^{\mathrm{t}}PPH = {}^{\mathrm{t}}HI_nH = {}^{\mathrm{t}}HH = nI_n$, donc PH est bien une matrice de Hadamard d'après la caractérisation de la question **2.**

- Pour tout $(i,j) \in [\![1\,;n]\!]^2$:

$$(DH)_{i,j}^2 = \Big(\sum_{k=1}^{n} D_{i,k}H_{k,j})^2 = D_{i,i}^2 H_{i,j}^2 = H_{i,j}^2 = 1$$

puisque $D_{i,k} = 0$ si $i \neq k$, et $D_{i,i} \in \{-1\,;1\}$. La matrice D, diagonale, est par ailleurs symétrique, et par produit de matrices diagonales dont les éléments appartiennent à $\{-1\,;1\}$, $D^2 = I_n$.

Par conséquent : ${}^{\mathrm{t}}(DH)DH = {}^{\mathrm{t}}H\,{}^{\mathrm{t}}DDH = {}^{\mathrm{t}}HD^2H = {}^{\mathrm{t}}HH = nI_n$, donc DH est une matrice de Hadamard.

- Pour tout $(i,j) \in [\![1\,;n]\!]$:

$$(HP)^2 = \Big(\sum_{k=1}^{n} H_{i,k}\delta_{k,\sigma(j)}\Big)^2 = H_{i,\sigma(j)}^2 = 1$$

et ${}^{\mathrm{t}}(HP)HP = {}^{\mathrm{t}}P\,{}^{\mathrm{t}}HHP = {}^{\mathrm{t}}PnI_nP = n\,{}^{\mathrm{t}}PP = nI_n$, donc HP est une matrice de Hadamard.

- Enfin, pour tout $(i,j) \in [\![1\,;n]\!]^2$:

$$(HD)^2 = \Big(\sum_{k=1}^{n} H_{i,k}D_{k,j}\Big)^2 = H_{i,j}^2 D_{j,j}^2 = H_{i,j}^2 = 1$$

et : ${}^{\mathrm{t}}(HD)HD = {}^{\mathrm{t}}D\,{}^{\mathrm{t}}HHD = DnI_nD = nD^2 = nI_n$, donc HD est une matrice de Hadamard.

5. Soit H une matrice de Hadamard de taille $n \times n$. Soit D la matrice diagonale dont les éléments diagonaux sont définis par : $\forall i \in [\![1\,;n]\!]$, $D_{i,i} = H_{1,i}$ qui appartient à $\{-1\,;1\}$.

D'après la question précédente, la matrice $H_0 = HD$ est une matrice de Hadamard, et :

$$\forall i \in [\![1\,;n]\!], \quad (HD)_{1,i} = \sum_{k=1}^{n} H_{1,k}D_{k,i} = H_{1,i}D_{i,i} = H_{1,i}^2 = 1,$$

donc la première ligne de cette matrice de Hadamard est bien $(1,`\cdots,1)$.

6. D'après la question **3.**, la matrice ${}^{\mathrm{t}}H_0$ est aussi une matrice de Hadamard, dont les éléments de la première colonne sont tous égaux à 1. Le produit scalaire de cette première colonne avec chacune des autres colonnes de ${}^{\mathrm{t}}H_0$ est alors simplement égal à la somme des éléments de cette colonne, qui valent tous 1 ou -1.

Or cette somme doit aussi être égale à 0 : c'est possible si et seulement si le nombre d'éléments égaux à -1 d'une colonne, est égal au nombre d'éléments de cette même colonne égaux à 1, et ceci n'est possible que si le nombre n d'éléments d'une colonne, est pair.

7. Soit $S \in \mathcal{M}_n(\mathbb{R})$ une matrice de Hadamard dont les éléments de la première ligne sont tous égaux à 1 ($\forall j \in [\![1\,;n]\!],\ S_{1,j} = 1$).

On sait alors que ${}^{\mathrm{t}}S$ est aussi une matrice de Hadamard, et comme on l'a vu à la question précédente, cela implique que la somme des éléments de chaque colonne de ${}^{\mathrm{t}}S$ autre que la première, est égale à 0, ce qui est équivalent au fait que la somme des éléments de chaque ligne de S autre que la première, est nulle.

Soit alors $(i,m) \in [\![2\,;n]\!]^2$ tel que $i \neq m$:

$$\sum_{k=1}^{n}(S_{i,k}+1)(S_{m,k}+1) = \sum_{k=1}^{n} S_{i,k} + \sum_{k=1}^{n} S_{i,k}S_{m,k} + \sum_{k=1}^{n} S_{m,k} + n.$$

Or $\displaystyle\sum_{k=1}^{n} S_{i,k} = \sum_{k=1}^{n} S_{m,k} = 0$ d'après ce qu'on a expliqué juste auparavant. Et $\displaystyle\sum_{k=1}^{n} S_{i,k}S_{m,k} = 0$ également, puisque cela correspond au produit scalaire des colonnes d'indices i et m de ${}^{\mathrm{t}}S$, qui est nul puisque $i \neq m$ et ${}^{\mathrm{t}}S$ est une matrice de Hadamard.

Ainsi, on a bien :

$$\forall (i,m) \in [\![2\,;n]\!]^2 \quad \text{tels que } i \neq m, \quad \sum_{k=1}^{n}(S_{i,k}+1)(S_{m,k}+1) = n.$$

8. Chaque coefficient $S_{i,k}$ ou $S_{m,k}$ vaut -1 ou 1, donc $(S_{i,k}+1)(S_{m,k}+1)$ est le produit de deux facteurs qui valent chacun 0 ou 2.

L'entier n peut être égal à 2 ; si $n \geqslant 3$, le résultat précédent implique que les termes non nuls de la somme précédente (il y en a forcément, puisque la somme vaut n) égaux à $2 \times 2 = 4$, donc n est un multiple de 4.

9. Soit $n > 2$: n doit être pair d'après **6.**. Soit H une matrice de Hadamard de taille $n \times n$. Une conséquence de la question **4.** est effectivement que la multiplication par -1 de certaines colonnes d'une matrice de Hadamard (qui revient à la multiplier à droite par une matrice diagonale D dont les éléments diagonaux sont égaux à 1 ou -1) donne encore une matrice de Hadamard, de même que la permutation de certaines colonnes (qui revient à une multiplication à droite par une matrice de permutation P).

Comme on l'a fait à la queston **5.**, on peut multiplier par -1 les colonnes de la matrice dont les éléments de la première ligne sont égaux à -1, et on obtient une matrice de Hadamard dont la première ligne est $(1, \cdots, 1)$.

On peut ensuite permuter les colonnes de la matrice, selon la valeur des éléments de sa deuxième ligne, de sorte que l'on regroupe à la fin de la première ligne, tous les éléments qui valent -1 ; le début de cette deuxième ligne ne contient que des éléments égaux à 1.

Ensuite : toujours par permutation des premières colonnes dont les deux premiers éléments sont égaux à 1, on peut regrouper sur les premières colonnes celles dont les éléments de la troisième ligne sont égaux à 1 : le deuxième groupe de colonnes est donc constitué de colonnes dont les trois premiers éléments sont dans cet ordre, $1, 1, -1$.

On procède ensuite de même pour le bloc de colonnes de la matrice dont les deux premiers éléments sont dans cet ordre, $1, -1$: par permutation, on regroupe ensemble les colonnes dont les trois premiers éléments sont égaux à $1, -1, 1$; le quatrième et dernier groupe de colonnes a ses trois premiers éléments égaux à $1, -1, -1$ dans cet ordre.

10. Appelons n_1, n_2, n_3, n_4 les tailles respectives des blocs de colonnes de la matrice de Hadamard précédemment construite.

Du fait que la transposée de cette matrice est encore une matrice de Hadamard, le produit scalaire des deux premières lignes de cette matrice doit être nul, ce qui donne la relation :

$$n_1 + n_2 - n_3 - n_4 = 0 \iff n_1 + n_2 = n_3 + n_4 \quad (R_1).$$

Par le même raisonnement concernant les lignes 1 et 3, et les lignes 2 et 3 de la matrice, on obtient :

$$n_1 + n_3 = n_2 + n_4 \quad (R_2) \quad \text{et} \quad n_1 + n_4 = n_2 + n_3 \quad (R_3).$$

L'opération $(R_1) - (R_2)$ donne : $n_2 - n_3 = n_3 - n_2 \iff n_2 - n_3 = 0 \iff n_2 = n_3$,
donc (R_1) donne aussi $n_1 = n_4$, et (R_3) devient alors $2n_1 = 2n_2 \iff n_1 = n_2$.

On obtient ainsi : $n_1 = n_2 = n_3 = n_4$, c'est-à-dire que les 4 blocs verticaux de la matrice précédemment construite, sont de même taille.

Ainsi, $n = n_1 + n_2 + n_3 + n_4 = 4n_1$ et on en déduit à nouveau que n est nécessairement divisible par 4.

11. Soient $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_k(\mathbb{R})$ deux matrices de Hadamard.

Par définition, les matrices A et B ont des coefficients tous égaux à 1 ou -1, donc il en est de même pour la matrice $A \otimes B$ par définition de celle-ci.

Notons par ailleurs $B_1, \dots, B_n$ les colonnes de la matrice B. Considérons deux colonnes différentes de la matrice $A \otimes B$, il y a deux cas de figure possibles :

- Soit ces deux colonnes appartiennent au même bloc de colonnes de $A \otimes B$, de la forme $\begin{pmatrix} A_{1,j}B \\ A_{2,j}B \\ \vdots \\ A_{n,j}B \end{pmatrix}$:
  cela signifie alors qu'il existe deux entiers $(k, \ell) \in [\![1\,;n]\!]^2$ tels que ces deux colonnes sont de la forme $\begin{pmatrix} A_{1,j}B_k \\ A_{2,j}B_k \\ \vdots \\ A_{n,j}B_k \end{pmatrix}$ et $\begin{pmatrix} A_{1,j}B_\ell \\ A_{2,j}B_\ell \\ \vdots \\ A_{n,j}B_\ell \end{pmatrix}$.
  Le produit scalaire de ces deux colonnes est alors :
  $$\sum_{i=1}^{n} A_{i,j}\, {}^{\mathrm{t}}B_k A_{i,j} B_\ell = \left(\sum_{i=1}^{n} \underbrace{A_{i,j}^2}_{=1} \right) \cdot \underbrace{{}^{\mathrm{t}}B_k B_\ell}_{=0} = 0.$$
- Soit ces deux colonnes appartiennent à des blocs de colonnes de $A \otimes B$ différents, de la forme $\begin{pmatrix} A_{1,j}B \\ A_{2,j}B \\ \vdots \\ A_{n,j}B \end{pmatrix}$ et $\begin{pmatrix} A_{1,m}B \\ A_{2,m}B \\ \vdots \\ A_{n,m}B \end{pmatrix}$: cela signifie alors qu'il existe deux entiers $(k, \ell) \in [\![1\,;n]\!]^2$ tels que ces deux colonnes sont de la forme $\begin{pmatrix} A_{1,j}B_k \\ A_{2,j}B_k \\ \vdots \\ A_{n,j}B_k \end{pmatrix}$ et $\begin{pmatrix} A_{1,m}B_\ell \\ A_{2,m}B_\ell \\ \vdots \\ A_{n,m}B_\ell \end{pmatrix}$.
  Le produit scalaire de ces deux colonnes est alors :
  $$\sum_{i=1}^{n} A_{i,j}\, {}^{\mathrm{t}}B_k A_{i,m}\, {}^{\mathrm{t}}B_\ell = \underbrace{\left(\sum_{i=1}^{n} A_{i,j} A_{i,m} \right)}_{=0} {}^{\mathrm{t}}B_k B_\ell$$
  puisque la somme $\displaystyle\sum_{i=1}^{n} A_{i,j} A_{i,m}$ correspond au produit scalaire, nul, des colonnes j et m de la matrice A.

Deux colonnes distinctes de la matrice $A \otimes B$ sont donc toujours orthogonales : il s'agit bien d'une matrice de Hadamard.

12. La matrice $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est une matrice de Hadamard d'ordre 2. La matrice $H_2 = H_1 \otimes H_1$ est donc, d'après ce qui précède, une matrice de Hadamard d'ordre $4 = 2^2$.

En définissant par récurrence, pour tout $n \in \mathbb{N}^*$, $H_{n+1} = H_n \otimes H_1$: une récurrence immédiate montre, grâce au résultat précédent, que pour tout $m \in \mathbb{N}^*$, H_m est une matrice de Hadamard de $\mathcal{M}_{2^m}(\mathbb{R})$.

13. La fonction `Python` ci-dessous réalise le travail demandé.

```
import numpy as np

def test_hadamard(M):
    n, p = np.shape(M)
    if n != p:
        return -2
    else:
        for i in range(0,n):
            for j in range(0,n):
                if M[i,j]**2 !=1 :
                    return -1
        for j in range(0,n-1):
            for k in range(j+1,n):
                if np.dot(np.transpose(M[:,j]),M[:,k]) != 0:
                    return 0
    return 1
```

Dans la deuxième double boucle `for`, on réalise le produit scalaire de chaque colonne j $(0 \leqslant j \leqslant n-2)$ avec chaque colonne k $(j+1 \leqslant k \leqslant n-1)$, c'est-à-dire qu'on calcule bien tous les produits scalaires de deux colonnes distinctes de H.

14. La fonction `Python` ci-dessous réalise le travail demandé :

```
import numpy.random as rd

def rand_hadam(m, Nmax):
    n = 4*m
    for tst in range(0, Nmax):
        matpm = np.ones((n, n), dtype = int)
        for i in range(0, n):
            nb_un = 0
            j = 0
            while 2*nb_un < n and j < n:
                val = rd.randint(0,2)
                nb_un += val
                matpm[i, j] = 2*val-1
                j = j+1
            if (2*nb_un == n):
                for k in range(j, n):
                    matpm[i, k] = -1
        if (test_hadamard(matpm)==1):
            return matpm
    return np.zeros((n, n), dtype = int)
```

Remarque : À l'exécution, ce programme s'avère assez inefficace : l'appel `rand_hadam(2, 100000)` ne parvient pas à générer une matrice de Hadamard aléatoire de taille 8, même en 100000 essais.

Partie II : variables aléatoires deux à deux indépendantes sur un espace probabilisé fini.

15. On vérifie les 4 points qui font de l'application $(x, y) \in \mathbb{R}^n \times \mapsto \langle x;\ y\rangle$, un produit scalaire sur $\mathbb{R}^n$. Notons d'abord qu'il s'agit bien d'une forme sur $\mathbb{R}^n$: $\forall (x, y) \in \mathbb{R}^n \times \mathbb{R}^n$, $\langle x;\ y\rangle$ est un réel comme somme de réels.

- Pour tous vecteurs x, y, z de $\mathbb{R}^n$ et pour tout réel λ :

$$\langle \lambda \cdot x + y;\ z\rangle = \sum_{k=1}^{n} p_k(\lambda x_k + y_k)z_k = \lambda \sum_{k=1}^{n} p_k x_k z_k + \sum_{k=1}^{n} p_k y_k z_k = \lambda\langle x;\ z\rangle + \langle y;\ z\rangle,$$

  ce qui prouve la linéarité par rapport à la première variable.

- Pour tous vecteurs x, y de $\mathbb{R}^n$:

$$\langle x;\ y\rangle = \sum_{k=1}^{n} p_k x_k y_k = \sum_{k=1}^{n} p_k y_k x_k = \langle y;\ x\rangle,$$

  ce qui prouve la symétrie.

- Pour tout vecteur x de $\mathbb{R}^n$: $\quad \langle x;\ x\rangle = \displaystyle\sum_{k=1}^{n} p_k x_k^2 \geqslant 0$, puisque les $(p_k)_{1\leqslant k\leqslant n}$ sont positifs en tant que probabilités, il s'agit donc d'une somme de réels positifs.

- Soit $x \in \mathbb{R}^n$; une somme de réels positifs est nulle si et seulement si chacun de ses termes est nul, donc :

$$\langle x;\ x\rangle = 0 \iff \forall k \in [\![1\,;n]\!],\ p_k x_k^2 = 0 \overset{(*)}{\iff} \forall k \in [\![1\,;n]\!],\ x_k = 0$$

  puisque par hypothèse, $p_k = \mathbf{P}(\{\omega_k\}) \neq 0$ pour tout entier k compris entre 1 et n.

L'application $\langle \cdot;\ \cdot\rangle$ est bien une forme bilinéaire symétrique, définie positive : c'est un produit scalaire sur $\mathbb{R}^n$.

16. Soit $i \in [\![1\,;\ell]\!]$. Comme l'univers Ω est fini, la variable aléatoire Z_i admet une espérance et une variance, et puisque Z_i n'est pas constante (vu que $Z_i(\Omega)$ contient au moins 2 valeurs distinctes), alors $\mathbf{V}(Z_i) \neq 0$ (et en fait $\mathbf{V}(Z_i) > 0$).

On cherche donc deux réels a_i et b_i avec $a_i > 0$ tels que :

$$\mathbf{V}(a_i Z_i + b_i) = 1 \iff a_i^2 \mathbf{V}(Z_i) = 1 \iff a_i = \frac{1}{\sqrt{\mathbf{V}(Z_i)}} = \frac{1}{\sigma(Z_i)} \text{ puisque } \sigma(Z_i) > 0,$$

et $\mathbf{E}(a_i Z_i + b_i) = 0 \iff a_i \mathbf{E}(Z_i) + b_i = 0 \iff b_i = -\dfrac{\mathbf{E}(Z_i)}{\sigma(Z_i)}$. Il existe bien un unique couple (a_i, b_i) de $\mathbb{R}_+^* \times \mathbb{R}$ qui vérifie les deux conditions imposées.

17. Soient V et W deux variables aléatoires réelles sur Ω.
On pose $v = \big(V(\omega_1), \ldots, V(\omega_n)\big) \in \mathbb{R}^n$, et $w = \big(W(\omega_1), \ldots, W(\omega_n)\big) \in \mathbb{R}^n$.

Par définition : $\quad \mathbf{E}(V) = \displaystyle\sum_{i=1}^{n} V(\omega_i)\mathbf{P}(\{\omega_i\}) = \sum_{i=1}^{n} v_i p_i = \sum_{i=1}^{n} p_i v_i \times 1 = \langle v;\ u_0\rangle$,

et : $\quad \mathbf{E}(VW) = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n} V(\omega_i)W(\omega_i)\mathbf{P}(\{\omega_i\}) = \sum_{i=1}^{n} p_i v_i w_i = \langle v;\ w\rangle$.

18. Des deux questions précédentes on déduit, pour tout $(i, j) \in [\![1\,;n]\!]^2$ tel que $i \neq j$:

$$\langle x_i;\ u_0\rangle = \mathbf{E}(X_i) = \mathbf{E}(a_i Z_i + b_i) = 0, \quad \langle x_i;\ x_i\rangle = \sum_{i=1}^{n} p_i x_i^2 = \mathbf{E}(X_i^2) = \mathbf{V}(X_i) + \mathbf{E}(X_i)^2 = 1,$$

$$\langle x_i;\ x_j\rangle = \mathbf{E}(X_i X_j) = \mathbf{E}(X_i)\mathbf{E}(X_j) = 0.$$

19. De la question précédente, il ressort que la famille de vecteurs $(u_0, x_1, \dots, x_n)$ est orthogonale, donc libre dans l'espace euclidien $\mathbb{R}^n$: cette famille compte donc au plus $n = \dim \mathbb{R}^n$ vecteurs, ce qui assure que $\ell + 1 \leqslant n$. L'énoncé suppose que $\ell \geqslant 2$, donc $\ell + 1 \geqslant 3$.

20. Soit Z une variable aléatoire réelle d'espérance nulle. On pose $z = \big(Z(\omega_1), \dots, Z(\omega_n)\big) \in \mathbb{R}^n$, et on suppose que $Z(\Omega) = \{\alpha_1, \dots, \alpha_m\}$ comprend au moins 3 valeurs distinctes.

a) Pour tout $k \in [\![1\,; m]\!]$, $\mathbf{P}(Z = \alpha_k) > 0$ et les $(\alpha_k)_{1 \leqslant k \leqslant m}$ sont deux à deux distincts, donc les vecteurs $V_1 = \big(\mathbf{P}(Z = \alpha_1), \dots, \mathbf{P}(Z = \alpha_m)\big)$ et $V_2 = \big(\alpha_1 \mathbf{P}(Z = \alpha_1), \dots, \alpha_m \mathbf{P}(Z = \alpha_m)\big)$ sont non nuls et non colinéaires.

Puisque $m \geqslant 3$, alors $\dim \big(\mathrm{Vect}(V_1, V_2)\big)^\perp \geqslant 1$, et il existe un vecteur $B = (\beta_1, \dots, \beta_m) \in \mathbb{R}^m$ non nul dans cet orthogonal, tel que :

$$\langle V_1;\ B\rangle = 0 \iff \sum_{k=1}^{m} \mathbf{P}(Z = \alpha_k)\beta_k = 0 \quad \text{et} \quad \langle V_2;\ B\rangle = 0 \iff \sum_{k=1}^{m} \mathbf{P}(Z = \alpha_k)\alpha_k\beta_k = 0.$$

b) L'application $T :\ Q \in \mathbb{R}_{m-1}[x] \mapsto \big(Q(\alpha_1), \dots, Q(\alpha_m)\big) \in \mathbb{R}^m$ est clairement linéaire. Comme $\dim \mathbb{R}_{m-1}[x] = m = \dim \mathbb{R}^m$, il suffit donc de montrer que T est injective, pour que ce soit un isomorphisme d'espaces vectoriels.

Or, pour $Q \in \mathbb{R}_{m-1}[x]$: $T(Q) = 0_{\mathbb{R}^m}$ si et seulement si $Q(\alpha_1) = 0 = \dots = Q(\alpha_m)$, c'est-à-dire si et seulement si Q admet au moins les m réels distincts $\alpha_1, \dots, \alpha_m$ comme racines.

Dans $\mathbb{R}_{m-1}[x]$, le seul polynôme qui possède au moins m racines distinctes est le polynôme nul, donc $T(Q) = 0_{\mathbb{R}^m} \iff Q = 0_{\mathbb{R}_{m-1}[x]}$.

L'application T est donc bien injective : c'est un isomorphisme d'espaces vectoriels.

c) Avec les notations des deux questions précédentes : il existe un unique polynôme $Q \in \mathbb{R}_{m-1}[x]$ tel que $T(Q) = B \iff \forall k \in [\![1\,; m]\!],\ Q(\alpha_k) = \beta_k$, de sorte qu'il existe un unique polynôme $Q \in \mathbb{R}_{m-1}[x]$ tel que :

$$\sum_{k=1}^{m} \mathbf{P}(Z = \alpha_k)\beta_k = 0 \iff \sum_{k=1}^{m} Q(\alpha_k)\mathbf{P}(Z = \alpha_k) = 0 \iff \mathbf{E}\big(Q(Z)\big) = 0$$

$$\text{et} \sum_{k=1}^{m} \mathbf{P}(Z = \alpha_k)\alpha_k\beta_k = 0 \iff \sum_{k=1}^{m} Q(\alpha_k)\alpha_k\mathbf{P}(Z = \alpha_k) = 0 \iff \mathbf{E}\big(Q(Z)Z\big) = 0,$$

où $Q(Z)(\Omega)$ est constitué des valeurs distinctes prises par les $(\beta_k)_{1 \leqslant k \leqslant m}$: d'après a), cet univers-image est bien non réduit à $\{0\}$.

21. L'énoncé appelle r le nombre de variables aléatoires X_i $(1 \leqslant i \leqslant \ell)$ dont l'univers-image contient au moins 3 valeurs distinctes.

a) Le résultat de la question **21.**c) peut, comme à la question **18.**, se traduire ainsi :

pour tout $i \in [\![1\,; \ell]\!]$ telle que $m_i = \# X_i(\Omega) > 2$, en notant $x_i = \big(X_i(\omega_1), \dots, X_i(\omega_n)\big) \in \mathbb{R}^n$, Q_i l'unique polynôme de $\mathbb{R}_{m_i - 1}[x]$ vérifiant les relations de **21.**c) et $q_i = \big(Q_i(X_i)(\omega_1), \dots, Q_i(X_i)(\omega_n)\big)$, alors $q_i \neq 0_{\mathbb{R}^{m_i}}$ et :

$$\langle q_i;\ u_0\rangle = 0, \quad \langle q_i;\ x_i\rangle 0$$

Soit par ailleurs $(i, j) \in [\![1\,; n]\!]^2$ avec $\# X_i(\Omega) > 2$ et $i \neq j$: par indépendance de X_i et X_j, d'après le lemme des coalitions, $Q_i(X_i)$ et X_j sont encore indépendantes, donc :

$$\mathbf{E}\big(Q_i(X_i)X_j\big) = \mathbf{E}\big(Q_i(X_i)\big) \times \underbrace{\mathbf{E}(X_j)}_{=0} = 0, \text{ ce qui se réécrit :} \quad \langle q_i;\ x_j\rangle = 0.$$

Ainsi, les vecteurs $\big\{x_i |\ 1 \leqslant i \leqslant \ell\big\} \cup \big\{q_i |\ i \in [\![1\,; \ell]\!] \text{ et } \# X_i(\Omega) > 2\big\} \cup \{u_0\}$ forment une famille orthogonale de vecteurs non nuls de $\mathbb{R}^n$: comme à la question **19.**, un argument de dimension donne :

$$\ell + r + 1 \neq n \iff r + \ell \leqslant n - 1.$$

b) Par définition, r est naturellement inférieur ou égal à ℓ, donc :

$$2r \leqslant r+\ell \leqslant n-1 \Longrightarrow r \leqslant \frac{n-1}{2}.$$

22. On suppose de plus dans cette question que $\ell = n-1$.

a) Cette hypothèse, rapprochée du résultat de **21.**a), implique nécessairement $r=0$, c'est-à-dire que pour tout $i \in [\![1\,;\ell]\!]$, $\#X_i(\Omega)=2$, puisque ces univers-images contiennent par principe au moins deux éléments distincts, et que ($r=0$) aucun d'entre eux ne contient strictement plus de deux éléments distincts.

b) Soit $i \in [\![1\,;n-1]\!]$.
Soient α_i et β_i deux réels tels que $X_i(\Omega)=\{\alpha_i,\beta_i\}$ avec $\alpha_i > \beta_i$, et soit $\theta_i \in]0\,;1[$ tel que :

$$\mathbf{P}(X_i=\alpha_i) \quad \text{et} \quad \mathbf{P}(X_i=\beta_i)=1-\theta_i.$$

On a toujours :

$$\mathbf{E}(X_i)=0 \iff \alpha_i\theta_i+\beta_i(1-\theta_i)=0 \quad \text{et} \quad \mathbf{V}(X_i)=1 \iff \mathbf{E}(X_i^2)=1 \iff \alpha_i^2\theta_i+\beta_i^2(1-\theta_i)=1,$$

ce qui donne :

$$\beta_i = -\frac{\theta_i}{1-\theta_i}\alpha_i \quad \text{et} \quad \alpha_i^2\theta_i+\frac{\theta_i^2}{1-\theta_i}\alpha_i^2=1 \iff \alpha_i^2\cdot\frac{\theta_i}{1-\theta_i}=1,$$

Si α_i, la plus grande des deux valeurs prises par X_i, était négatif (ou nul), alors X_i ne pourrait pas être nulle (somme de deux termes négatifs, dont un au moins strictement négatif), donc nécessairement $\alpha_i > 0 > \beta_i$, et par conséquent les dernières relations obtenues donnent :

$$\alpha_i = \sqrt{\frac{1-\theta_i}{\theta_i}} \quad \text{et} \quad \beta_i = -\frac{\theta_i}{1-\theta_i}\sqrt{\frac{1-\theta_i}{\theta_i}} = -\sqrt{\frac{\theta_i}{1-\theta_i}} = -\frac{1}{\alpha_i}.$$

c) Montrons que la matrice MD est orthogonale en calculant $MD\times {}^{\mathrm{t}}(MD) = MD\,{}^{\mathrm{t}}D\,{}^{\mathrm{t}}M$ $= MD^2\,{}^{\mathrm{t}}M$, où D est une matrice diagonale, par conséquent symétrique, et D^2 est la matrice diagonale d'éléments diagonaux $p_1,\dots,p_n$.

La matrice MD^2 a pour coefficients $(MD^2)_{i,j} = \begin{cases} X_i(\omega_j)p_j \text{ si } i \leqslant n-1 \\ p_j \text{ si } i=n \end{cases}$.

La matrice $MD^2\,{}^{\mathrm{t}}M$ a alors pour coefficients :

$$(MD^2\,{}^{\mathrm{t}}M)_{i,j} = \begin{cases} \sum\limits_{k=1}^{n} X_i(\omega_k)X_j(\omega_k)p_k & \text{si } i \leqslant n-1 \text{ et } j \leqslant n-1 \\ \sum\limits_{k=1}^{n} X_j(\omega_k)p_k & \text{si } i=n \text{ et } j \leqslant n-1 \\ \sum\limits_{k=1}^{n} p_k & \text{si } i=j=n \end{cases} = \begin{cases} \mathbf{E}(X_iX_j) & \text{si } i \leqslant n-1 \text{ et } j \leqslant n-1 \\ \mathbf{E}(X_j) & \text{si } i=n \text{ et } j \leqslant n-1 \\ 1 & \text{si } i=j=n \end{cases}.$$

Or par hypothèse : si $i \neq j$ (avec $1 \leqslant i,j \leqslant n-1$), alors X_i et X_j sont indépendantes, donc $\mathbf{E}(X_iX_j)=\mathbf{E}(X_i)\mathbf{E}(X_j)=0\times 0=0$.
Si par contre $1 \leqslant i=j \leqslant n-1$, alors $\mathbf{E}(X_iX_j)=\mathbf{E}(X_i^2)=\mathbf{V}(X_i)=1$ puisque $\mathbf{E}(X_i)=0$.
Enfin si $i=n$ et $j \leqslant n-1$, le coefficient vaut $\mathbf{E}(X_j)=0$, de sorte que finalement :

$$\forall (i,j) \in [\![1\,;n]\!]^2, \quad (MD^2\,{}^{\mathrm{t}}M)_{i,j} = \begin{cases} 1 & \text{si } i=j \\ 0 & \text{si } i \neq j \end{cases},$$

donc $MD\,{}^{\mathrm{t}}(MD)=I_n$, ce qui prouve que MD est une matrice orthogonale.

d) Soit Y la variable aléatoire définie par : $\forall j \in [\![1\,;n]\!],\ Y(\omega_j) = \dfrac{1}{p_j}$.

Comme MD est orthogonale, on a aussi ${}^{\mathrm{t}}(MD)MD = I_n$. Or la matrice MD a pour coefficients $(MD)_{i,j} = \begin{cases} X_i(\omega_j)\sqrt{p_j} & \text{si } i \neq n-1 \\ \sqrt{p_j} & \text{si } i = n \end{cases}$, donc la matrice ${}^{\mathrm{t}}(MD)MD$ a pour coefficients :

$$\forall (i,j) \in [\![1\,;n]\!], \quad \big({}^{\mathrm{t}}(MD)MD\big)_{i,j} = \Big(\sum_{k=1}^{n-1} X_k(\omega_i)X_k(\omega_j) + 1\Big)\sqrt{p_ip_j}.$$

Ainsi, pour tout $i \in [\![1\,;n]\!]$: $\big({}^{\mathrm{t}}(MD)MD\big)_{i,i} = \Big(1 + \sum_{k=1}^{n-1} X_k^2(\omega_i)\Big)p_i$, mais ce coefficient diagonal doit aussi être égal à 1, de sorte que :

$$\forall i \in [\![1\,;n]\!],\ 1 + \sum_{k=1}^{n} X_k^2(\omega_i) = \frac{1}{p_i}, \text{ soit : } \quad \forall i \in [\![1\,;n]\!],\ 1 + \sum_{k=1}^{n} X_k^2(\omega_i) = Y(\omega_i),$$

ce qui prouve l'égalité de variables aléatoires : $\quad Y = 1 + \displaystyle\sum_{k=1}^{n} X_k^2$.

e) Soit $i \in [\![1\,;n-1]\!]$. D'après ce qui précède : $X_iY = X_i + \displaystyle\sum_{k=1}^{n-1} X_iX_k^2$, et ces deux variables aléatoires ont la même espérance.

Or $\mathbf{E}(X_iY) = \displaystyle\sum_{k=1}^{n} X_i(\omega_k)Y(\omega_k)p_k = \sum_{k=1}^{n} X_i(\omega_k)\frac{1}{p_k}p_k = \sum_{k=1}^{n} X_i(\omega_k)$.

Par ailleurs, et par linéarité de l'espérance :

$$\mathbf{E}\Big(1 + \sum_{k=1}^{n-1} X_iX_k^2\Big) = \underbrace{\mathbf{E}(X_i)}_{=0} + \sum_{k=1}^{n-1}\mathbf{E}(X_iX_k^2) \overset{(*)}{=} \sum_{\substack{1\leqslant k\leqslant n-1 \\ k\neq i}} \underbrace{\mathbf{E}(X_i)}_{=0}\mathbf{E}(X_k^2) + \mathbf{E}(X_i^3) = \mathbf{E}(X_i^3)$$

$(*)$ toujours par indépendance de X_i et X_k si $i \neq k$.

On a bien démontré : $\quad \mathbf{E}(X_i^3) = \displaystyle\sum_{k=1}^{n} X_i(\omega_k)$.

f) On reprend les notations de la question 22.b) et on pose :

$$\forall i \in [\![1\,;n-1]\!], \quad m_i = \#\big\{k \in [\![1\,;n]\!] \big|\ X_i(\omega_k) = \alpha_i\big\}.$$

D'après la relation obtenue en **22.**e), et sachant que X_i ne prend que les deux valeurs α_i et $\beta_i = -\dfrac{1}{\alpha_i}$:

$$\mathbf{E}(X_i^3) = \sum_{k=1}^{n} X_i(\omega_k) = m_i\alpha_i + (n - m_i)\beta_i.$$

Le théorème de transfert donen par ailleurs : $\quad \mathbf{E}(X_i^3) = \alpha_i^3\theta_i + \beta_i^3(1-\theta_i)$.

Or, d'après la relation obtenue en **22.**b) :

$$\alpha_i^2 = \frac{1-\theta_i}{\theta_i} = \frac{1}{\theta_i} - 1 \iff \theta_i = \frac{1}{1+\alpha_i^2}, \text{ et } 1 - \theta_i = 1 - \frac{1}{1+\alpha_i^2} = \frac{\alpha_i^2}{1+\alpha_i^2},$$

de sorte que :

$$\mathbf{E}(X_i^3) = \alpha_i^3\theta_i + \beta_i^3(1-\theta_i) = \frac{\alpha_i^3}{1+\alpha_i^2} - \frac{1}{\alpha_i^3}\cdot\frac{\alpha_i^2}{1+\alpha_i^2} = \frac{\alpha_i^4 - 1}{\alpha_i(1+\alpha_i^2)} = \frac{(\alpha_i^2+1)(\alpha_i^2-1)}{\alpha_i(1+\alpha_i^2)} = \alpha_i - \frac{1}{\alpha_i}.$$

En identifiant ces deux expressions de la même espérance $\mathbf{E}(X_i^3)$, on obtient l'égalité :

$$m_i\alpha_i - \frac{n-m_i}{\alpha_i} = \alpha_i - \frac{1}{\alpha_i} \iff m_i\alpha_i^2 - (n-m_i) = \alpha_i^2 - 1,$$

ce qui donne finalement :

$$n - m_i - 1 = (m_i-1)\alpha_i^2 \iff \alpha_i = \sqrt{\frac{n-m_i-1}{m_i-1}} \text{ et } \theta_i = \frac{1}{\alpha_i^2+1} = \frac{1}{1+\frac{n-m_i-1}{m_i-1}} = \frac{m_i-1}{n-2} \quad (A_1)$$

Par hypothèse faite au début de la partie actuelle :

$$0 < \theta_i < 1 \iff 0 < \frac{m_i-1}{n-2} < 1 \iff 0 < m_i - 1 < n-2 \iff 1 < m_i < n-1 \iff 2 \leqslant m_i \leqslant n-2 \quad (A_3)$$

puisque m_i est un entier naturel.

Cette dernière relation implique aussi : $\quad n-2 \geqslant 2 \iff n \geqslant 4 \quad (A_2)$.

g) On suppose dans cette question que pour tout $i \in [\![1\,;n]\!]$, $p_i = \dfrac{1}{n}$.

(a) On a alors :

$$\theta_i = \mathbf{P}(X_i = \alpha_i) = \sum_{\substack{k\in[\![1\,;n]\!] \\ \text{tq } X_i(\omega_k)=\alpha_i}} p_k = \frac{\#\big\{k \in [\![1\,;n]\!] \mid X_i(\omega_k) = \alpha_i\big\}}{n} = \frac{m_i}{n},$$

mais on a aussi $\theta_i = \dfrac{m_i-1}{n-2}$ (A_1), donc :

$$\frac{m_i}{n} = \frac{m_i-1}{n-2} \iff nm_i - 2m_i = nm_i - n \iff n = 2m_i,$$

qui implique bien que n est pair, et que $\theta_i = \dfrac{m_i}{n} = \dfrac{m_i}{2m_i} = \dfrac{1}{2}$.

(b) Les éléments de la matrice M sont les $X_i(\omega_j)$ qui valent α_i ou β_i, mis à part les coefficients de la dernière ligne qui sont tous égaux à 1.

Sachant désormais que $\theta_i = \frac{1}{2}$, alors d'après **22.**b), $\alpha_i = \sqrt{\dfrac{1-\frac{1}{2}}{\frac{1}{2}}} = 1$ et $\beta_i = -\frac{1}{\alpha_i} = -1$, donc les coefficients de M sont tous égaux à 1 ou -1.

Par ailleurs, on sait aussi d'après **22.**c) que :

$${}^{\mathrm{t}}(MD)MD = I_n \iff D\,{}^{\mathrm{t}}MMD = I_n \iff {}^{\mathrm{t}}MM = D^{-2}.$$

La matrice D^2 est diagonale, et a pour éléments diagonaux les réels $\dfrac{1}{(\sqrt{p_i})^2} = \dfrac{1}{p_i} = n$,
donc ${}^{\mathrm{t}}MM = nI_n$.

Ceci achève de prouver, d'après la caractérisation de la question **2.**, que M est une matrice de Hadamard.

Partie III : deux propriétés des matrices de Hadamard

23. La linéarité de l'application $\varphi : \begin{array}{ccc} \mathbb{R}^{n^2} & \to & \mathcal{M}_n(\mathbb{R}) \\ (x_1,\ldots,x_{n^2}) & \mapsto & \big[x_{(i-1)n+j}\big]_{(i,j)\in[\![1\,;n]\!]^2} \end{array}$ est assez évidente :

Pour tous vecteurs $x = (x_1,\ldots,x_{n^2})$ et $y = (y_1,\ldots,y_{n^2})$ de $\mathbb{R}^{n^2}$ et tout réel λ,

$$\varphi(\lambda\cdot x+y) = \big[\lambda\cdot x_{(i-1)n+j} + y_{(i-1)n+j}\big]_{(i,j)\in[\![1\,;n]\!]^2} = \lambda\cdot\big[x_{(i-1)n+j}\big]_{(i,j)\in[\![1\,;n]\!]^2} + \big[y_{(i-1)n+j}\big]_{(i,j)\in[\![1\,;n]\!]^2} = \lambda\cdot\varphi(x)+\varphi(y).$$

Par ailleurs, pour tout vecteur $x = (x_1, \ldots, x_{n^2})$ de $\mathbb{R}^{n^2}$:

$$\begin{aligned}||\varphi(x)||^2 &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_{(i-1)n+j}^2 = \sum_{j=1}^{n} x_j^2 + \sum_{j=1}^{n} x_{n+j}^2 + \sum_{j=1}^{n} x_{2n+j} + \cdots + \sum_{j=1}^{n} x_{n(n-1)+j}^2 \\ &= \sum_{j=1}^{n} x_j^2 + \sum_{j=n+1}^{2n} x_j^2 + \sum_{j=2n+1}^{3n} x_j^2 + \cdots + \sum_{j=n^2-n+1}^{n^2} x_j^2 \\ &= \sum_{j=1}^{n^2} x_j^2 = ||x||^2,\end{aligned}$$

ce qui donne bien, par positivité de la norme : $\quad \forall x \in \mathbb{R}^{n^2},\ ||\varphi(x)|| = ||x||$.

24. Pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$:

$$||A||^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^2 = \sum_{j=1}^{n}\sum_{i=1}^{n} ({}^{\mathrm{t}}A)_{j,i} A_{i,j} = \sum_{j=1}^{n} ({}^{\mathrm{t}}AA)_{j,j} = \mathrm{Tr}({}^{\mathrm{t}}AA).$$

25. Soit $A \in \mathcal{M}_n(\mathbb{R})$.

Pour tout $i \in [\![1\,;n]\!]$:

$$\Big(\sum_{j=1}^{n} |A_{i,j}|\Big)^2 = \sum_{j=1}^{n} A_{i,j}^2 + \sum_{\substack{1\leqslant j,k\leqslant n \\ j\neq k}} |A_{i,j}|\cdot|A_{i,k}| \geqslant \sum_{j=1}^{n} A_{i,j}^2,$$

donc, par croissance de la fonction racine carrée sur $\mathbb{R}^+$:

$$\forall i \in [\![1\,;n]\!],\ \sqrt{\sum_{j=1}^{n} A_{i,j}^2} \leqslant \sum_{j=1}^{n} |A_{i,j}| \Longrightarrow \sum_{i=1}^{n}\Big(\sum_{j=1}^{n} A_{i,j}^2\Big) \leqslant \sum_{i=1}^{n}\sum_{j=1}^{n} |A_{i,j}| = F(A)$$

par sommation des inégalités.

Ensuite : la somme $\displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n} |A_{i,j}|$ peut apparaître comme le produit scalaire des vecteurs

$$a = \big(|A_{1,1}|, |A_{1,2}|, \ldots, |A_{1,n}|, \ldots, |A_{n,1}|, \ldots, |A_{n,n}|\big) \quad \text{et} \quad u = (1, 1, \ldots, 1) \text{ de } \mathbb{R}^{n^2};$$

L'inégalité de Cauchy-Schwarz avec le produit scalaire canonique sur cet espace s'écrit alors :

$$\begin{aligned}|\langle a\,, u\rangle| \leqslant ||a||\cdot||u|| &\iff \sum_{1\leqslant i,j\leqslant n} |A_{i,j}| \leqslant \sqrt{\sum_{1\leqslant i,j\leqslant n} 1^2}\cdot\sqrt{\sum_{1\leqslant i,j\leqslant n} A_{i,j}^2} \\ &\iff F(A) \leqslant \sqrt{n^2}\cdot\sqrt{\sum_{1\leqslant i,j\leqslant n} A_{i,j}^2} = n\Big(\sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^2\Big)^{1/2}.\end{aligned}$$

26. On pose $\mathscr{K}_n = \{x \in \mathbb{R}^{n^2} \,\big|\, \varphi(x) \in \mathscr{O}_n\}$.

Pour tout couple $(i,j) \in [\![1\,;n]\!]^2$, on pose $\varphi_{i,j} :\ x = (x_1, \ldots, x_{n^2}) \in \mathbb{R}^{n^2} \mapsto \big({}^{\mathrm{t}}(\varphi(x))\varphi(x)\big)_{i,j}$.

Pour tout $x = (x_1, \ldots, x_{n^2}) \in \mathbb{R}^{n^2}$, on a :

$$\varphi_{i,j}(x) = \sum_{k=1}^{n} {}^{\mathrm{t}}(\varphi(x)_{i,k}\varphi(x)_{k,j} = \sum_{k=1}^{n} x_{(k-1)n+i}x_{(k-1)n+j},$$

donc $\varphi_{i,j} : \ \mathbb{R}^{n^2} \to \mathbb{R}$ est une fonction continue sur $\mathbb{R}^{n^2}$ comme fonction polynômiale en les composantes de x.

Les équivalences :

$$\varphi(x) \in \mathscr{O}_n \iff {}^{\mathrm{t}}(\varphi(x))\varphi(x) = I_n \iff \Big(\forall i \in [\![1\,;n]\!],\ \varphi_{i,i}(x) = 1 \text{ et } \forall (i,j) \in [\![1\,;n]\!]^2 \text{ avec } i \neq j,\ \varphi_{i,j}(x) = 0\Big)$$

permettent d'écrire $\mathscr{K}_n$ comme l'ensemble :

$$\bigcap_{i=1}^{n} \{x \in \mathbb{R}^{n^2} \,|\, \varphi_{i,i}(x) \leqslant 1\} \cap \bigcap_{i=1}^{n} \{x \in \mathbb{R}^{n^2} \,|\, \varphi_{i,i}(x) \geqslant 1\} \cap \bigcap_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} \{x \in \mathbb{R}^{n^2} \,|\, \varphi_{i,j}(x) \leqslant 1\} \cap \bigcap_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} \{x \in \mathbb{R}^{n^2} \,|\, \varphi_{i,j}(x) \geqslant 1\}$$

Sous cette forme, $\mathscr{K}_n$ apparaît comme une intersection finie de parties fermées élémentaires de $\mathbb{R}^{n^2}$: c'est donc une partie fermée de $\mathbb{R}^{n^2}$.

Ensuite : pour tout $x \in \mathscr{K}_n$, $||x|| = ||\varphi(x)|| = \sqrt{\mathrm{Tr}({}^{\mathrm{t}}(\varphi(x))\varphi(x))} \overset{\varphi(x) \in \mathscr{O}_n}{=} \sqrt{\mathrm{Tr}(I_n)} = \sqrt{n}$, ce qui prouve que $\mathscr{K}_n$ est une partie bornée de $\mathbb{R}^{n^2}$.

27. Soit $(x, y) \in (\mathbb{R}^{n^2})^2$:

$$\begin{aligned}
\big|F\big(\varphi(x)\big) - F\big(\varphi(y)\big)\big| &= \left|\sum_{i=1}^{n}\sum_{j=1}^{n} \big(|\varphi(x)|_{i,j}| - |\varphi(y)_{i,j}|\big)\right| \\
&\leqslant \sum_{i=1}^{n}\sum_{j=1}^{n} \big||\varphi(x)|_{i,j} - |\varphi(y)|_{i,j}\big| \quad \text{d'après l'inégalité triangulaire} \\
&\leqslant \sum_{i=1}^{n}\sum_{j=1}^{n} |\varphi(x)_{i,j} - \varphi(y)_{i,j}| \quad \text{inégalité triangulaire renversée} \\
&\leqslant F\big(\varphi(x) - \varphi(y)\big) = F\big(\varphi(x-y)\big) \quad \text{par linéarité de } \varphi \\
&\leqslant n||\varphi(x-y)|| \quad \text{d'après } \textbf{25.} \\
&\leqslant n||x-y|| \quad \text{d'après } \textbf{23.}
\end{aligned}$$

28. La fonction $F \circ \varphi : \ \mathbb{R}^{n^2} \to \mathbb{R}$ est continue sur $\mathbb{R}^{n^2}$: on peut le justifier en considérant que F est une fonction polynômiale en les coordonnées de $x \in \mathbb{R}^{n^2}$.

Sinon, on peut utiliser l'inégalité de la question précédente en revenant à la définition de la continuité d'une fonction de plusieurs variables, à valeurs réelles :

Pour tout $\varepsilon > 0$, on peut définir $\alpha = \frac{\varepsilon}{n} > 0$, qui vérifie :

$$||x-y|| < \alpha \overset{n>0}{\iff} n||x-y|| < \varepsilon \overset{\textbf{27.}}{\Longrightarrow} \big|F\big(\varphi(x)\big) - F\big(\varphi(y)\big)\big| < \varepsilon,$$

ce qui correspond à la définition de la continuité de $F \circ \varphi$ sur $\mathbb{R}^{n^2}$.

Or $\mathscr{K}_n$ est d'après **26.** un fermé borné de $\mathbb{R}^{n^2}$: d'après le théorème des "bornes atteintes", la fonction $F \circ \varphi$ admet un maximum et un minimum sur $\mathbb{R}^{n^2}$:

$$\exists\ (x_0, y_0) \in (\mathbb{R}^{n^2})^2\,;\ \forall x \in \mathbb{R}^{n^2}, \quad F\big(\varphi(y_0)\big) \leqslant F\big(\varphi(x)\big) \leqslant F\big(\varphi(x_0)\big).$$

Or d'après la question **23.**, $\varphi : \ \mathbb{R}^{n^2} \to \mathcal{M}_n(\mathbb{R})$ est une application linéaire, vérifiant :

$$\forall x \in \mathbb{R}^{n^2},\ x \in \mathrm{Ker}(\varphi) \iff \varphi(x) = 0_{\mathcal{M}_n(\mathbb{R})} \iff ||\varphi(x)|| = 0 \iff ||x|| = 0 \iff x = 0_{\mathbb{R}^{n^2}},$$

donc φ est injective : comme $\dim \mathbb{R}^{n^2} = n^2 = \dim \mathcal{M}_n(\mathbb{R})$, alors φ est un isomorphisme d'espaces vectoriels, de sorte que : $\forall M \in \mathscr{O}_n(\mathbb{R}),\ \exists!\ x \in \mathbb{R}^{n^2}\,; M = \varphi(x)$, de sorte que :

$$\forall M \in \mathscr{O}_n(\mathbb{R}),\ F\big(M\big) \overset{x=\varphi^{-1}(M)}{=} F\big(\varphi(x)\big) \leqslant F\big(\varphi(x_0)\big)\big),$$

ce qui prouve, puisque $\varphi(x_0) \in \mathscr{O}_n(\mathbb{R})$, que F admet un maximum global sur $\mathscr{O}_n(\mathbb{R})$; de même, F admet un minimum global sur $\mathscr{O}_n(\mathbb{R})$ (atteint en $\varphi(y_0)$).

Dans toute la suite, on note M_n^- (respectivement M_n^+) la valeur minimale (respectivement maximale) de F sur $\mathscr{O}_n$:

$$M_n^- = \min_{Q\in\mathscr{O}_n} F(Q), \quad M_n^+ = \max_{Q\in\mathscr{O}_n} F(Q).$$

29. L'inégalité de gauche de (1) obtenue en **25.** s'écrit, pour $A \in \mathscr{O}_n$:

$$\sum_{i=1}^n \Big(\sum_{j=1}^n A_{i,j}\, {}^{\mathrm{t}}\!A_{j,i}\Big)^{1/2} \leqslant F(A) \iff \sum_{i=1}^n \big(\underbrace{A\, {}^{\mathrm{t}}\!A}_{=I_n}\big)_{i,i}^2 \leqslant F(A) \iff \sum_{i=1}^n 1 = n \leqslant F(A).$$

Ce minorant est atteint, puisque I_n est orthogonale et $F(I_n) = n$ comme somme des valeurs absolues de tous les coefficients de I_n. Ainsi, $M_n^- = n$.

30. On peut reprendre ici une partie du travail réalisé à la question **25.** : pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$, on a : $\forall i \in [\![$, $\Big(\sum\limits_{j=1}^n A_{i,j}^2\Big)^{1/2} \leqslant \sum\limits_{j=1}^n |A_{i,j}|$, et $\sum\limits_{j=1}^n A_{i,j}^2 = 1$ si de plus A est orthogonale.

Par conséquent, pour $Q \in \mathscr{O}_n$:

$$F(Q) = n \iff \sum_{i=1}^n\sum_{j=1}^n |Q_{i,j}| = \sum_{i=1}^n \Big(\sum_{j=1}^n Q_{i,j}^2\Big)^{1/2} \iff \forall i \in [\![1\,;n]\!],\ \sum_{j=1}^n Q_{i,j}^2 = \Big(\sum_{j=1}^n |Q_{i,j}|\Big)^2$$

$$\iff \forall i \in [\![1\,;n]\!],\ \sum_{\substack{1\leqslant j\leqslant n\\ j\neq i}} |Q_{i,j}| = 0 \iff \forall (i,j) \in [\![1\,;n]\!]^2 \text{ tels que } i \neq j,\ Q_{i,j} = 0$$

$$\iff Q \text{ est diagonale et orthogonale} \iff Q \text{ est diagonale et } Q^2 = I_n$$

$$\iff Q \text{ est diagonale et ses éléments diagonaux sont tous égaux à 1 ou } -1$$

31. Soit Q une matrice de $\mathscr{O}_n$. Les formules dans les espaces euclidiens donnent, en notant ici $\langle\cdot\,,\cdot\rangle$ le produit scalaire canonique sur $\mathcal{M}_n(\mathbb{R})$:

$$\begin{aligned}||Q - \frac{1}{\sqrt{n}}\mathbb{S}(Q)||^2 &= ||Q||^2 + \frac{1}{n}||\mathbb{S}(Q)||^2 - \frac{2}{\sqrt{n}}\langle Q\,,\mathbb{S}(Q)\rangle\\ &= \mathrm{Tr}({}^{\mathrm{t}}QQ) + \frac{1}{n}\sum_{i=1}^n\sum_{j=1}^n \underbrace{\big(\mathbb{S}(Q)\big)_{i,j}^2}_{=1} - \frac{2}{\sqrt{n}}\sum_{i=1}^n\sum_{j=1}^n Q_{i,j}\mathbb{S}(Q)_{i,j}\\ &= \mathrm{Tr}(I_n) + \frac{1}{n}\times n^2 - \frac{2}{\sqrt{n}}\underbrace{\sum_{i=1}^n\sum_{j=1}^n |Q_{i,j}|}_{=F(Q)} = 2n - \frac{2}{\sqrt{n}}F(Q),\end{aligned}$$

donc : $\quad \dfrac{2}{\sqrt{n}}F(Q) = 2n - ||Q - \dfrac{1}{\sqrt{n}}\mathbb{S}(Q)||^2 \iff F(Q) = n\sqrt{n} - \dfrac{\sqrt{n}}{2}||Q - \dfrac{1}{\sqrt{n}}\mathbb{S}(Q)||^2.$

32. Une norme étant toujours positive, le résultat précédent assure que : $\forall Q \in \mathscr{O}_n,\ F(Q) \leqslant n\sqrt{n}$, en particulier pour la matrice orthogonale en laquelle F atteint son maximum : $M_n^+ \leqslant n\sqrt{n}$.

L'égalité est, toujours d'après la question précédente, réalisée si et seulement s'il existe au moins une matrice orthogonale Q qui vérifie :

$$||Q - \frac{1}{\sqrt{n}}\mathbb{S}(Q)|| = 0 \iff \sqrt{n}Q = \mathbb{S}(Q).$$

Si une telle matrice Q existe, alors $H = \mathbb{S}(Q)$ est une matrice de $\mathcal{M}_n(\mathbb{R})$ dont tous les éléments sont égaux à 1 ou -1, et qui vérifie : ${}^{\mathrm{t}}HH = \sqrt{n}\,{}^{\mathrm{t}}Q \times \sqrt{n}Q = n\,{}^{\mathrm{t}}QQ = nI_n$, donc c'est une matrice de Hadamard.

Réciproquement : s'il existe une matrice de Hadamard H dans $\mathcal{M}_n(\mathbb{R})$, alors $Q = \frac{1}{\sqrt{n}}H$ est orthogonale : ${}^{\mathrm{t}}QQ = \frac{1}{n}\,{}^{\mathrm{t}}HH = \frac{1}{n} \cdot nI_n = I_n$, et $\mathbb{S}(Q) = H$ donc $Q = \frac{1}{\sqrt{n}}\mathbb{S}(Q) \iff F(Q) = n\sqrt{n}$.

33. Si n n'est pas un multiple de 4, sachant que $n \geqslant 3$, alors d'après **8.**, il ne peut pas exister de matrice de Hadamard d'ordre n ; et d'après le résultat précédent, le cas d'égalité dans **32.** ne se produit jamais : $\quad M_n^+ < n\sqrt{n}$.

34. On suppose dans cette question que $n = 3$. Pour tous réels α et β, on pose

$$U(\alpha, \beta) = \begin{pmatrix} \alpha & \beta & \beta \\ \beta & \alpha & -\beta \\ -\beta & \beta & -\alpha \end{pmatrix}.$$

La matrice $U(\alpha, \beta)$ appartient à $_3$ si et seulement si ses colonnes forment une famille orthonormée, ce qui est équivalent au système non linéaire d'inconnues α et β (en éliminant les équations redondantes) :

$$\begin{cases} \alpha^2 + 2\beta^2 & = 1 \\ 2\alpha\beta - \beta^2 & = 0 \end{cases} \iff \begin{cases} \alpha^2 + 2\beta^2 & = 1 \\ \beta(2\alpha - \beta) & = 0 \end{cases} \iff \begin{cases} \alpha^2 & = 1 \\ \beta & = 0 \end{cases} \text{ou} \begin{cases} 9\alpha^2 = 1 \\ \beta = 2\alpha \end{cases},$$

d'après la règle du produit nul. Les quatre matrices solutions sont donc :

$$U(1,0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ U(-1,0) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$U\big(\tfrac{1}{3}, \tfrac{2}{3}\big) = \begin{pmatrix} 1/3 & 2/3 & 2/3 \\ 2/3 & 1/3 & -1/3 \\ -2/3 & 2/3 & -1/3 \end{pmatrix} \text{ et } U\big(-\tfrac{1}{3}, -\tfrac{2}{3}\big) = \begin{pmatrix} -1/3 & -2/3 & -2/3 \\ -2/3 & -1/3 & 2/3 \\ 2/3 & -2/3 & 1/3 \end{pmatrix}.$$

Il reste donc à calculer les images par F de ces 4 matrices orthogonales, ce qui revient à additionner les valeurs absolues de tous leurs coefficients :

$$F\big(U(1,0)\big) = 3 = F\big(U(-1,0)\big) \quad \text{et} \quad F\Big(U\big(\tfrac{1}{3}, \tfrac{2}{3}\big)\Big) = 3 \times \frac{1}{3} + 6 \times \frac{2}{3} = 1 + 4 = 5 = F\Big(U\big(-\tfrac{1}{3}, -\tfrac{2}{3}\big)\Big).$$

On en déduit donc que : $\quad 5 \leqslant M_3^+ < 3\sqrt{3}$ (puisque 3 n'est pas un multiple de 4).

35. On suppose dans cette question que n est pair.

a) Soient $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ deux vecteurs de $\mathbb{R}^n$ dont toutes les composantes valent 1 ou -1, et qui ne sont pas orthogonaux.

Dans ce cas, $|\langle x\,;y\rangle| = \left|\sum_{i=1}^{n} x_i y_i\right|$ est une somme de n termes valant chacun 1 ou -1, qui ne s'annule pas : au pire, un maximum de termes égaux à 1 sont compensés par un nombre équivalent de termes égaux à -1 ; comme n est pair, il ne reste après simplification que des termes de même signe sous la valeur absolue, en nombre pair et non nul, ce qui implique bien : $\quad |\langle x\,;y\rangle| \geqslant 2$.

b) Soient x, y, u et v quatre vecteurs de $\mathbb{R}^n$. En remarquant que :

$$\langle x\,;y\rangle - \langle u\,;v\rangle = \langle y\,;x\rangle - \langle y\,;u\rangle + \langle y\,;u\rangle - \langle v\,;u\rangle = \langle y\,;x-u\rangle + \langle u\,;y-v\rangle,$$

et puisque pour tout réels a et b : $(a+b)^2 - 2(a^2+b^2) = -a^2 + 2ab - b^2 = -(a-b)^2 \leqslant 0$, alors $(a+b)^2 \leqslant 2(a^2+b^2)$ et :

$$\big(\langle x\,;y\rangle - \langle u\,;v\rangle\big)^2 = \big(\langle y\,;x-u\rangle + \langle u\,;y-v\rangle\big)^2 \leqslant 2\big(\langle y\,;x-u\rangle^2 + \langle u\,;y-v\rangle^2\big).$$

L'inégalité de Cauchy-Schwarz donnant :
$|\langle y\,;x-u\rangle| \leqslant ||y||\cdot||x-u|| \iff \langle y\,;x-u\rangle^2 \leqslant ||y||^2||x-u||^2$ et de même, $\langle u\,;y-v\rangle^2 \leqslant ||u||^2||y-v||^2$,

alors on a bien :

$$\big|\langle x\,;y\rangle - \langle u\,;v\rangle\big|^2 \leqslant 2\big(||y||^2||x-u||^2 + ||u||^2||y-v||^2\big),$$

d'où le résultat demandé par croissance de la fonction racine carrée sur $\mathbb{R}^+$.

c) Soit $Q \in \mathscr{O}_n$ telle que $\mathbb{S}(Q)$ n'est pas de Hadamard.
On cherche à minorer $||Q - \dfrac{1}{\sqrt{n}}\mathbb{S}(Q)||^2 = \dfrac{1}{n}||\sqrt{n}Q - \mathbb{S}(Q)||^2$ par $\dfrac{2}{n^2}$.
Comme la matrice $\mathbb{S}(Q)$ a des coefficients tous égaux à 1 ou -1, la seule façon pour elle de ne pas être de Hadamard, est d'avoir deux colonnes non orthogonales.
Notons x et y ces deux colonnes, assimilées à des vecteurs de $\mathbb{R}^n$, et notons u et v les deux colonnes de mêmes places dans la matrice Q.
alors $\langle u\,;v\rangle = 0$ (produit scalaire dans $\mathbb{R}^n$ puisque Q est orthogonale, et $|\langle x\,;y\rangle| \geqslant 2$ d'après la question a), puisque les deux vecteurs x et y vérifient les hypothèses menant à ce résultat.
On peut donc écrire, d'après le résultat de la question précédente :

$$2 \leqslant |\langle x\,;y\rangle| = |\langle x\,;y\rangle - n\langle u\,;v\rangle| = |\langle x\,;y\rangle - \rangle\sqrt{n}u\,;\sqrt{n}v\rangle| \leqslant \sqrt{2(||y||^2||x-\sqrt{n}u||^2 + n||u||^2||y-\sqrt{n}v||^2)}.$$

Or $||y||^2 = n$ puisque y ne contient que des éléments égaux à 1 ou -1, et $||u|| = 1$ puisque u est une colonne de la matrice orthogonale Q, donc :

$$2 \leqslant \sqrt{2n\big(||x-\sqrt{n}u||^2 + ||y-\sqrt{n}v||^2\big)} \iff \frac{2}{n} \leqslant ||x-\sqrt{n}u||^2 + ||y-\sqrt{n}v||^2.$$

Il reste à constater qu'avec la norme dans $\mathcal{M}_n(\mathbb{R})$:

$$||\sqrt{n}Q - \mathbb{S}(Q)||^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}\big(\sqrt{n}Q_{i,j} - \mathbb{S}(Q)_{i,j}^2\big) = \sum_{j=1}^{n}||s_j - \sqrt{n}q_j||^2$$

où s_j représente la j-ième colonne de $\mathcal{S}(Q)$, et q_j la j-ième colonne de Q, la norme qui est appliquée à $s_j - \sqrt{n}q_j$ étant dans ce cas celle sur $\mathbb{R}^n$.
L'entier n étant pair et supérieur ou égal à 3, on peut alors naturellement écrire, puisque x et y (resp. u et v) sont des colonnes s_j de $\mathcal{S}(Q)$ (resp. des colonnes q_j de Q) :

$$\frac{2}{n} \leqslant ||x-\sqrt{n}u||^2 + ||y-\sqrt{n}v||^2 \leqslant \sum_{j=1}^{n}||s_j-\sqrt{n}q_j||^2 \Longrightarrow \frac{2}{n} \leqslant ||\mathbb{S}(Q)-\sqrt{n}Q||^2 = n||Q - \frac{1}{\sqrt{n}}\mathbb{S}(Q)||^2$$

$$\Longrightarrow \frac{2}{n^2} \leqslant ||Q - \frac{1}{\sqrt{n}}\mathbb{S}(Q)||^2.$$

d) D'après la question précédente et la question **31.** : s'il n'existe aucune matrice de Hadamard dans $\mathcal{M}_n(\mathbb{R})$, alors pour toute matrice orthogonale $Q \in \mathscr{O}_n$,

$$F(Q) = n\sqrt{n} - \frac{\sqrt{n}}{2}||Q - \frac{1}{\sqrt{n}}\mathbb{S}(Q)||^2 \leqslant n\sqrt{n} - \frac{\sqrt{n}}{2} \times \frac{2}{n^2} = n\sqrt{n} - \frac{1}{n\sqrt{n}},$$

et cette inégalité reste vraie pour la matrice Q en laquelle F atteint son maximum, ce qui donne bien :

$$M_n^+ \leqslant n\sqrt{n} - \frac{1}{n\sqrt{n}}.$$

★★★ FIN DU SUJET ★★★