

HEC–ESSEC – Mathématiques I

Mathématiques approfondies

Corrigé du sujet adapté – 2024

Les questions et sous-questions conservent la numérotation de l'énoncé. Les notations $\mathbb{E}$ et $\mathbb{V}$ désignent l'espérance et la variance. La transposée d'une matrice A est notée ${}^tA$. Pour $A \in \mathcal{M}_{n,m}(\mathbb{R})$, $A_{i,j}$ est le coefficient en ligne i et colonne j .

Partie I – Existence des matrices de Hadamard

Partie I – Matrices de permutation, de Hadamard et produit $\otimes$

$H \in \mathcal{M}_n(\mathbb{R})$ ($n \geq 2$) est une matrice de Hadamard, de colonnes $c_1, \dots, c_n$ et de lignes $\ell_1, \dots, \ell_n$. Une matrice de permutation associée à une bijection σ vérifie $P_{i,j} = \delta_{i,\sigma(j)}$. Questions 1 à 14.

Corrigé – Partie I.

1. Matrices de permutation.

Soit σ la bijection associée à P . Pour $(j, k) \in \llbracket 1; n \rrbracket^2$,

$$({}^tPP)_{j,k} = \sum_{i=1}^n P_{i,j}P_{i,k} = \sum_{i=1}^n \delta_{i,\sigma(j)}\delta_{i,\sigma(k)} = \delta_{\sigma(j),\sigma(k)} = \delta_{j,k},$$

la dernière égalité venant de l'injectivité de σ . Donc ${}^tPP = I_n$. Ensuite, pour tout (i, j) ,

$$({}^tP)_{i,j} = P_{j,i} = \delta_{j,\sigma(i)} = \delta_{\sigma^{-1}(j),i} = \delta_{i,\sigma^{-1}(j)},$$

car $j = \sigma(i) \iff i = \sigma^{-1}(j)$. Comme σ^{-1} est une bijection de $\llbracket 1; n \rrbracket$,

$$P \in \mathcal{O}_n \quad \text{et} \quad {}^tP \text{ est la matrice de permutation associée à } \sigma^{-1}.$$

2. Caractérisation des matrices de Hadamard.

Notons $q_1, \dots, q_n$ les colonnes de Q . Pour tout (j, k) ,

$$({}^tQQ)_{j,k} = \sum_{i=1}^n Q_{i,j}Q_{i,k} = {}^tq_j q_k.$$

$\Rightarrow$ Si Q est de Hadamard, ses coefficients valent ± 1 , donc $Q_{i,j}^2 = 1$. Pour $j \neq k$, ${}^tq_j q_k = 0$ par orthogonalité des colonnes, et ${}^tq_j q_j = \sum_{i=1}^n Q_{i,j}^2 = n$. Donc ${}^tQQ = nI_n$.

$\Leftarrow$ Si $Q_{i,j}^2 = 1$ pour tout (i, j) , alors $Q_{i,j} \in \{-1, 1\}$. Si de plus ${}^tQQ = nI_n$, les coefficients non diagonaux sont nuls : ${}^tq_j q_k = 0$ pour $j \neq k$. Les colonnes sont deux à deux orthogonales.

$$Q \text{ de Hadamard} \iff {}^tQQ = nI_n \text{ et } \forall (i, j), Q_{i,j}^2 = 1.$$

3. La transposée de H .

D'après la question 2, ${}^tHH = nI_n$, donc ${}^t\left(\frac{1}{\sqrt{n}}H\right)\frac{1}{\sqrt{n}}H = I_n$. La matrice carrée $\frac{1}{\sqrt{n}}H$ admet donc $\frac{1}{\sqrt{n}}{}^tH$ comme inverse à gauche, donc comme inverse : $\frac{1}{\sqrt{n}}H \cdot \frac{1}{\sqrt{n}}{}^tH = I_n$, c'est-à-dire

$${}^t({}^tH){}^tH = H{}^tH = nI_n.$$

Les coefficients de tH sont ceux de H et vérifient donc $({}^tH)_{i,j}^2 = 1$. La question 2 donne

tH est de Hadamard : les lignes $\ell_1, \dots, \ell_n$ sont deux à deux orthogonales.

4. Stabilité par permutation et changements de signe.

La matrice D vérifie ${}^tDD = D^2 = I_n$ (ses coefficients diagonaux valent ± 1) : elle est orthogonale, comme P (question 1). Si $R \in \mathcal{O}_n$, alors

$${}^t(RH)(RH) = {}^tH{}^tRRH = {}^tHH = nI_n.$$

- Coefficients de PH : $(PH)_{i,j} = \sum_k \delta_{i,\sigma(k)} H_{k,j} = H_{\sigma^{-1}(i),j} \in \{-1, 1\}$.
- Coefficients de DH : $(DH)_{i,j} = D_{i,i} H_{i,j} \in \{-1, 1\}$.

Par la question 2, PH et DH sont de Hadamard. Pour HP et HD : tH est de Hadamard (question 3), ${}^tP$ est une matrice de permutation (question 1) et ${}^tD = D$. Ce qui précède appliqué à tH montre que ${}^tP{}^tH = {}^t(HP)$ et $D{}^tH = {}^t(HD)$ sont de Hadamard. La question 3 appliquée à ces matrices donne que leurs transposées HP et HD le sont aussi.

PH, DH, HP, HD sont des matrices de Hadamard.

On retiendra que $(HP)_{i,j} = \sum_k H_{i,k} \delta_{k,\sigma(j)} = H_{i,\sigma(j)}$: la j -ième colonne de HP est $c_{\sigma(j)}$. Multiplier à droite par P permute donc les colonnes, et multiplier à droite par D change le signe de certaines colonnes.

5. Une matrice de Hadamard de première ligne $(1, \dots, 1)$.

Soit $D = \text{diag}(H_{1,1}, \dots, H_{1,n})$, diagonale à coefficients ± 1 . Alors

$$(HD)_{1,j} = H_{1,j} D_{j,j} = H_{1,j}^2 = 1.$$

D'après la question 4,

$S = HD$ est une matrice de Hadamard dont la première ligne est $(1, \dots, 1)$.

6. Parité de n .

Soit S comme à la question 5. D'après la question 3 appliquée à S , ses lignes sont deux à deux orthogonales ; comme $n \geq 2$, la deuxième ligne existe et

$$0 = \sum_{k=1}^n S_{1,k} S_{2,k} = \sum_{k=1}^n S_{2,k}.$$

Si a désigne le nombre de coefficients égaux à 1 dans la deuxième ligne, cette somme vaut $a - (n - a) = 2a - n$. Ainsi $n = 2a$:

n est pair, et chaque ligne $i \geq 2$ de S contient $n/2$ coefficients égaux à 1.

(Le même calcul vaut pour toute ligne $i \geq 2$.)

7. Une identité sur les lignes de S .

Par la question 3, les lignes de S sont deux à deux orthogonales. Pour $i \neq m$ dans $\llbracket 2; n \rrbracket$, les indices 1, i , m sont distincts, et on développe :

$$\sum_{k=1}^n (S_{i,k} + 1)(S_{m,k} + 1) = \underbrace{\sum_k S_{i,k} S_{m,k}}_{=0} + \underbrace{\sum_k S_{i,k} S_{1,k}}_{=0} + \underbrace{\sum_k S_{m,k} S_{1,k}}_{=0} + \sum_k 1,$$

en utilisant $S_{1,k} = 1$. D'où

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

8. $n = 2$ ou n multiple de 4.

Si $n \neq 2$, alors $n \geq 3$, donc $n \geq 4$ puisque n est pair. On applique la question 7 avec $i = 2$, $m = 3$. Chaque facteur $S_{i,k} + 1$ vaut 0 ou 2, donc chaque terme $(S_{2,k} + 1)(S_{3,k} + 1)$ vaut 0 ou 4. En notant $b = \#\{k \mid S_{2,k} = S_{3,k} = 1\}$, on obtient $n = 4b$.

$$\boxed{n = 2 \quad \text{ou} \quad n \equiv 0 \pmod{4}.}$$

9. Forme normale des trois premières lignes.

On suppose $n > 2$, donc $n \geq 4$ (question 8) et la troisième ligne existe. Partons de la matrice S de la question 5. D'après la question 6, sa deuxième ligne contient $n/2$ coefficients égaux à 1 et $n/2$ égaux à -1 .

- Soit σ_1 une bijection de $\llbracket 1; n \rrbracket$ telle que $S_{2,\sigma_1(j)} = 1$ pour $j \leq n/2$ et $S_{2,\sigma_1(j)} = -1$ pour $j > n/2$. Avec P_1 la matrice de permutation associée, $T_1 = SP_1$ est de Hadamard (question 4), ses colonnes sont $c_{\sigma_1(1)}, \dots, c_{\sigma_1(n)}$ (remarque de la question 4) : sa première ligne vaut toujours $(1, \dots, 1)$ et sa deuxième ligne est $(1, \dots, 1, -1, \dots, -1)$.
- Soit σ_2 une bijection qui laisse stables $\llbracket 1; n/2 \rrbracket$ et $\llbracket n/2 + 1; n \rrbracket$, et qui, à l'intérieur de chacun de ces deux ensembles, place d'abord les colonnes de T_1 dont le troisième coefficient vaut 1, puis celles dont il vaut -1 . Avec P_2 la matrice associée, $T = T_1 P_2$ est de Hadamard.

La permutation σ_2 ne mélange pas les deux moitiés, donc les deux premières lignes de T sont celles de T_1 , et la troisième ligne est rangée comme voulu.

$$\boxed{T = SP_1 P_2 \text{ est de Hadamard et ses trois premières lignes ont la forme demandée.}}$$

Notons a, b, c, d les nombres de colonnes des quatre blocs (de gauche à droite).

10. Les quatre blocs ont la même taille.

Les lignes de T sont deux à deux orthogonales (question 3), et les trois premières lignes donnent :

$$\begin{cases} a + b + c + d = n & (\text{nombre de coefficients de la ligne 1}) \\ a + b - c - d = 0 & (\text{lignes 1 et 2}) \\ a - b + c - d = 0 & (\text{lignes 1 et 3}) \\ a - b - c + d = 0 & (\text{lignes 2 et 3}) \end{cases}$$

En additionnant les quatre équations : $4a = n$. Puis $a + b = n/2$, $a + c = n/2$ donnent $b = c = n/4$, et enfin $d = n - a - b - c = n/4$.

$$a = b = c = d = \frac{n}{4}, \quad \text{donc } 4 \mid n.$$

11. Produit $A \otimes B$.

Soient $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_k(\mathbb{R})$ de Hadamard. Par construction par blocs, pour $(i, j) \in \llbracket 1; n \rrbracket^2$ et $(p, q) \in \llbracket 1; k \rrbracket^2$,

$$(A \otimes B)_{(i-1)k+p, (j-1)k+q} = A_{i,j} B_{p,q} \in \{-1, 1\}.$$

Toute ligne (resp. colonne) de $A \otimes B$ s'écrit de façon unique $(i-1)k+p$ (resp. $(j-1)k+q$). Pour deux colonnes d'indices (j, q) et (j', q') :

$$\sum_{i=1}^n \sum_{p=1}^k A_{i,j} B_{p,q} A_{i,j'} B_{p,q'} = \left(\sum_{i=1}^n A_{i,j} A_{i,j'} \right) \left(\sum_{p=1}^k B_{p,q} B_{p,q'} \right) = n \delta_{j,j'} \cdot k \delta_{q,q'},$$

d'après la question 2 appliquée à A et à B . Ainsi ${}^t(A \otimes B)(A \otimes B) = nk I_{nk}$ et la question 2 donne

$$A \otimes B \text{ est une matrice de Hadamard de taille } nk.$$

12. Existence en taille 2^m .

La matrice $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est de Hadamard : ses coefficients valent ± 1 et ses colonnes vérifient $1 \cdot 1 + 1 \cdot (-1) = 0$. Montrons par récurrence sur $m \in \mathbb{N}^*$ qu'il existe une matrice de Hadamard $H_{2^m} \in \mathcal{M}_{2^m}(\mathbb{R})$. L'initialisation est H_2 . Si H_{2^m} existe, la question 11 montre que $H_2 \otimes H_{2^m}$ est de Hadamard de taille $2 \cdot 2^m = 2^{m+1}$.

$$\forall m \in \mathbb{N}^*, \exists H_{2^m} \in \mathcal{M}_{2^m}(\mathbb{R}) \text{ de Hadamard, par exemple } H_{2^{m+1}} = H_2 \otimes H_{2^m}.$$

13. Fonction `test_hadamard`.

On teste d'abord le caractère carré, puis on parcourt tous les coefficients ($M_{i,j}^2 = 1$ équivaut à $M_{i,j} \in \{-1, 1\}$), enfin on calcule le produit scalaire de chaque couple de colonnes distinctes $j < k$.

```
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):
            for k in range(j+1, n):
                if np.dot(M[:,j], M[:,k]) != 0:
                    return 0
    return 1
```

$$\text{blancs : } n \neq p, n, n, M[i,j]**2, n, j+1, M[:,j], M[:,k].$$

14. Fonction rand_hadam.

La première ligne reste égale à $(1, \dots, 1)$ (initialisation par `np.ones`), on remplit donc les lignes $i \geq 1$ (indices Python). Dans la boucle `while`, `nb_un` compte les 1 déjà placés et `j-nb_un` compte les -1 ; on s'arrête dès que l'un des deux atteint $n/2$. La variable `val` vaut 0 ou 1 et le coefficient placé est $2\text{val} - 1 \in \{-1, 1\}$, donc `nb_un` augmente de `val`. Si ce sont les 1 qui ont atteint $n/2$, on complète par des -1 ; sinon les coefficients restants valent déjà 1 grâce à l'initialisation.

```
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(1, n):
            nb_un = 0
            j = 0
            while 2*nb_un < n and 2*(j-nb_un) < 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)
```

blancs : 1, 2*(j-nb_un), val, j+1, -1, matpm.

Les deux conditions de la boucle garantissent $j = \text{nb_un} + (j - \text{nb_un}) < n$, donc l'indice `j` reste valide.

Partie II – Variables aléatoires deux à deux indépendantes

Partie II – Espace probabilisé fini et orthogonalité

$\Omega = \{\omega_1, \dots, \omega_n\}$, $p_k = \mathbb{P}(\{\omega_k\}) > 0$, $\langle u; v \rangle = \sum_{k=1}^n p_k u_k v_k$ et $u_0 = (1, \dots, 1)$. Les variables $Z_1, \dots, Z_\ell$ ($\ell \geq 2$) sont deux à deux indépendantes et prennent chacune au moins deux valeurs. Questions 15 à 22.

Corrigé – Partie II.

15. Un produit scalaire sur $\mathbb{R}^n$.

L'application est symétrique ($p_k x_k y_k = p_k y_k x_k$) et linéaire par rapport à la première variable, donc bilinéaire par symétrie. Elle est positive : $\langle x; x \rangle = \sum_k p_k x_k^2 \geq 0$. Elle est définie : pour tout k , $p_k = \mathbb{P}(\{\omega_k\}) > 0$ car $\{\omega_k\}$ est non vide ; si $\langle x; x \rangle = 0$, la somme de termes positifs $p_k x_k^2$ est nulle, donc chaque $x_k = 0$.

$$\langle \cdot; \cdot \rangle \text{ est un produit scalaire sur } \mathbb{R}^n.$$

16. Centrage et réduction.

La variable Z_i est finie, donc admet espérance et variance. Montrons d'abord $\mathbb{V}(Z_i) > 0$. On a $\mathbb{V}(Z_i) = \sum_{k=1}^n p_k (Z_i(\omega_k) - \mathbb{E}(Z_i))^2$; si elle était nulle, comme les p_k sont strictement positifs, on aurait $Z_i(\omega_k) = \mathbb{E}(Z_i)$ pour tout k , donc $\#Z_i(\Omega) = 1$, ce qui est exclu.

Pour $(a, b) \in \mathbb{R}^* \times \mathbb{R}$, par linéarité de l'espérance et $\mathbb{V}(aZ_i + b) = a^2 \mathbb{V}(Z_i)$:

$$\mathbb{E}(aZ_i + b) = 0 \iff b = -a\mathbb{E}(Z_i), \quad \mathbb{V}(aZ_i + b) = 1 \iff a^2 = \frac{1}{\mathbb{V}(Z_i)}.$$

Avec la condition $a > 0$, on obtient un unique couple :

$$a_i = \frac{1}{\sqrt{\mathbb{V}(Z_i)}}, \quad b_i = -\frac{\mathbb{E}(Z_i)}{\sqrt{\mathbb{V}(Z_i)}}.$$

17. Espérances et produit scalaire.

L'univers étant fini, en regroupant les ω_k selon la valeur prise par V ,

$$\mathbb{E}(V) = \sum_{x \in V(\Omega)} x \mathbb{P}(V = x) = \sum_{x \in V(\Omega)} x \sum_{k: V(\omega_k) = x} p_k = \sum_{k=1}^n p_k V(\omega_k) = \sum_{k=1}^n p_k v_k \cdot 1.$$

Le produit VW est une variable aléatoire dont le vecteur des valeurs est $(v_1 w_1, \dots, v_n w_n)$; la formule précédente lui donne $\mathbb{E}(VW) = \sum_k p_k v_k w_k$.

$$\mathbb{E}(V) = \langle v; u_0 \rangle, \quad \mathbb{E}(VW) = \langle v; w \rangle.$$

18. Relations d'orthogonalité.

D'après les questions 16 et 17 :

- $\langle x_i; u_0 \rangle = \mathbb{E}(X_i) = 0$;
- $\langle x_i; x_i \rangle = \mathbb{E}(X_i^2) = \mathbb{V}(X_i) + \mathbb{E}(X_i)^2 = 1$;

- pour $i \neq j$, Z_i et Z_j sont indépendantes, donc $X_i = a_i Z_i + b_i$ et $X_j = a_j Z_j + b_j$ le sont aussi (fonctions de variables indépendantes). Ainsi $\langle x_i; x_j \rangle = \mathbb{E}(X_i X_j) = \mathbb{E}(X_i) \mathbb{E}(X_j) = 0$.

$$\langle x_i; u_0 \rangle = 0, \quad \langle x_i; x_i \rangle = 1, \quad \langle x_i; x_j \rangle = 0 \ (i \neq j).$$

19. Encadrement de ℓ .

De plus $\langle u_0; u_0 \rangle = \sum_k p_k = 1$. La famille $(u_0, x_1, \dots, x_\ell)$ est donc orthonormée dans l'espace euclidien $(\mathbb{R}^n, \langle \cdot; \cdot \rangle)$, donc libre. Elle contient $\ell + 1$ vecteurs d'un espace de dimension n , et $\ell \geq 2$:

$$3 \leq \ell + 1 \leq n.$$

20. Un polynôme orthogonal à 1 et à Z .

- a) L'application $\psi : \beta \in \mathbb{R}^m \mapsto \left(\sum_k \mathbb{P}(Z = \alpha_k) \beta_k, \sum_k \mathbb{P}(Z = \alpha_k) \alpha_k \beta_k \right) \in \mathbb{R}^2$ est linéaire. Par le théorème du rang, $\dim \text{Ker } \psi = m - \text{rg } \psi \geq m - 2 \geq 1$ car $m > 2$. Un vecteur non nul de $\text{Ker } \psi$ convient :

$$\exists (\beta_1, \dots, \beta_m) \neq 0, \quad \sum_{k=1}^m \mathbb{P}(Z = \alpha_k) \beta_k = 0, \quad \sum_{k=1}^m \mathbb{P}(Z = \alpha_k) \alpha_k \beta_k = 0.$$

- b) T est linéaire : $(\lambda Q + \mu R)(\alpha_k) = \lambda Q(\alpha_k) + \mu R(\alpha_k)$. Si $T(Q) = 0$, le polynôme Q , de degré au plus $m - 1$, admet les m racines distinctes $\alpha_1, \dots, \alpha_m$, donc $Q = 0$: T est injective. Comme $\dim \mathbb{R}_{m-1}[x] = m = \dim \mathbb{R}^m$, T est bijective.

$$T \text{ est un isomorphisme de } \mathbb{R}_{m-1}[x] \text{ sur } \mathbb{R}^m.$$

- c) Soit $Q = T^{-1}(\beta_1, \dots, \beta_m)$, de sorte que $Q(\alpha_k) = \beta_k$. Par le théorème de transfert,

$$\mathbb{E}(Q(Z)) = \sum_{k=1}^m Q(\alpha_k) \mathbb{P}(Z = \alpha_k) = \sum_{k=1}^m \beta_k \mathbb{P}(Z = \alpha_k) = 0,$$

$$\mathbb{E}(Q(Z)Z) = \sum_{k=1}^m Q(\alpha_k) \alpha_k \mathbb{P}(Z = \alpha_k) = \sum_{k=1}^m \alpha_k \beta_k \mathbb{P}(Z = \alpha_k) = 0.$$

Chaque α_k est une valeur prise par Z , donc $Q(Z)(\Omega) = \{\beta_1, \dots, \beta_m\}$, qui contient un réel non nul.

$$\exists Q \in \mathbb{R}_{m-1}[x], \quad \mathbb{E}(Q(Z)) = 0, \quad \mathbb{E}(Q(Z)Z) = 0, \quad Q(Z)(\Omega) \neq \{0\}.$$

21. Majoration du nombre de variables à plus de deux valeurs.

- a) Soit $I = \{i \in \llbracket 1; \ell \rrbracket \mid \#X_i(\Omega) > 2\}$, de cardinal r . Pour $i \in I$, X_i est d'espérance nulle et prend $m_i > 2$ valeurs ; la question 20 fournit un polynôme Q_i tel que $\mathbb{E}(Q_i(X_i)) = 0$, $\mathbb{E}(Q_i(X_i)X_i) = 0$ et $Q_i(X_i) \neq 0$. Notons $y_i = (Q_i(X_i)(\omega_1), \dots, Q_i(X_i)(\omega_n))$. D'après la question 17 :

- $\langle y_i; u_0 \rangle = \mathbb{E}(Q_i(X_i)) = 0$ et $\langle y_i; x_i \rangle = \mathbb{E}(Q_i(X_i)X_i) = 0$;
- pour $j \neq i$, $Q_i(X_i)$ et X_j sont indépendantes (fonctions de Z_i et de Z_j), donc $\langle y_i; x_j \rangle = \mathbb{E}(Q_i(X_i)) \mathbb{E}(X_j) = 0$;
- pour $i \neq i'$ dans I , de même $\langle y_i; y_{i'} \rangle = \mathbb{E}(Q_i(X_i)) \mathbb{E}(Q_{i'}(X_{i'})) = 0$;

- $y_i \neq 0$ car $Q_i(X_i)(\Omega) \neq \{0\}$.

Avec la question 18, la famille $(u_0, x_1, \dots, x_\ell, (y_i)_{i \in I})$ est une famille orthogonale de $1 + \ell + r$ vecteurs non nuls de $\mathbb{R}^n$, donc libre. Ainsi $1 + \ell + r \leq n$:

$$\ell + r \leq n - 1.$$

- b) Comme $I \subset \llbracket 1; \ell \rrbracket$, $r \leq \ell$, donc $2r \leq \ell + r \leq n - 1$:

$$r \leq \frac{n - 1}{2}.$$

22. Le cas extrémal $\ell = n - 1$.

- a) Avec $\ell = n - 1$, la question 21.a donne $r \leq 0$, donc $r = 0$: $\#X_i(\Omega) \leq 2$ pour tout i .
Par ailleurs $x \mapsto a_i x + b_i$ est injective ($a_i \neq 0$), donc $\#X_i(\Omega) = \#Z_i(\Omega) \geq 2$.

$$\forall i \in \llbracket 1; n - 1 \rrbracket, \#X_i(\Omega) = 2.$$

- b) Les conditions $\mathbb{E}(X_i) = 0$ et $\mathbb{E}(X_i^2) = 1$ s'écrivent

$$\theta_i \alpha_i + (1 - \theta_i) \beta_i = 0, \quad \theta_i \alpha_i^2 + (1 - \theta_i) \beta_i^2 = 1.$$

La première donne $\beta_i = -\frac{\theta_i}{1 - \theta_i} \alpha_i$. En reportant :

$$\theta_i \alpha_i^2 + \frac{\theta_i^2}{1 - \theta_i} \alpha_i^2 = \frac{\theta_i(1 - \theta_i) + \theta_i^2}{1 - \theta_i} \alpha_i^2 = \frac{\theta_i}{1 - \theta_i} \alpha_i^2 = 1, \quad \text{donc} \quad \alpha_i^2 = \frac{1 - \theta_i}{\theta_i}.$$

Comme $\theta_i/(1 - \theta_i) > 0$, α_i et β_i sont de signes opposés (et non nuls car distincts) ;

avec $\alpha_i > \beta_i$, on a $\alpha_i > 0$. Enfin $\beta_i = -\frac{\theta_i}{1 - \theta_i} \sqrt{\frac{1 - \theta_i}{\theta_i}} = -\sqrt{\frac{\theta_i}{1 - \theta_i}}$.

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

- c) $(MD)_{i,j} = M_{i,j} \sqrt{p_j}$. Notons $m^{(i)}$ la i -ième ligne de M , vue comme vecteur de $\mathbb{R}^n$: $m^{(i)} = x_i$ pour $i \leq n - 1$ et $m^{(n)} = u_0$. Pour tout (i, i') ,

$$(MD {}^t(MD))_{i,i'} = \sum_{j=1}^n p_j M_{i,j} M_{i',j} = \langle m^{(i)}; m^{(i')} \rangle = \delta_{i,i'},$$

d'après la question 18 et $\langle u_0; u_0 \rangle = 1$. Donc $MD {}^t(MD) = I_n$; la matrice carrée MD est inversible d'inverse ${}^t(MD)$, d'où aussi ${}^t(MD)MD = I_n$.

$$MD \in \mathcal{O}_n.$$

- d) Le coefficient diagonal (j, j) de ${}^t(MD)MD = D {}^tMM D = I_n$ s'écrit

$$p_j \sum_{i=1}^n M_{i,j}^2 = 1, \quad \text{soit} \quad 1 + \sum_{k=1}^{n-1} X_k(\omega_j)^2 = \frac{1}{p_j} = Y(\omega_j).$$

Ceci valant pour tout j , $Y = 1 + \sum_{k=1}^{n-1} X_k^2$. Calculons alors $\mathbb{E}(X_i Y)$ de deux façons. D'une part, $\mathbb{E}(X_i Y) = \sum_j p_j X_i(\omega_j) \frac{1}{p_j} = \sum_j X_i(\omega_j)$. D'autre part, par linéarité, puis indépendance de X_i et X_k^2 pour $k \neq i$,

$$\mathbb{E}(X_i Y) = \mathbb{E}(X_i) + \mathbb{E}(X_i^3) + \sum_{k \neq i} \mathbb{E}(X_i) \mathbb{E}(X_k^2) = \mathbb{E}(X_i^3).$$

$$Y = 1 + \sum_{k=1}^{n-1} X_k^2, \quad \mathbb{E}(X_i^3) = \sum_{k=1}^n X_i(\omega_k).$$

e) Les affirmations (A1), (A2), (A3).

Fixons i et notons $\alpha = \alpha_i$, $\theta = \theta_i$, $m = m_i$. D'après 22.b, $\alpha^2 = \frac{1-\theta}{\theta}$, donc $\theta = \frac{1}{1+\alpha^2}$ et $1-\theta = \frac{\alpha^2}{1+\alpha^2}$. Alors

$$\mathbb{E}(X_i^3) = \theta \alpha^3 - (1-\theta) \frac{1}{\alpha^3} = \frac{\alpha^3}{1+\alpha^2} - \frac{1}{\alpha(1+\alpha^2)} = \frac{\alpha^4 - 1}{\alpha(1+\alpha^2)} = \alpha - \frac{1}{\alpha}.$$

Par ailleurs, X_i vaut α en m points et $-1/\alpha$ aux $n-m$ autres, donc $\sum_k X_i(\omega_k) = m\alpha - \frac{n-m}{\alpha}$. La question 22.d donne, après multiplication par α :

$$\alpha^2 - 1 = m\alpha^2 - (n-m), \quad \text{soit} \quad \alpha^2(m-1) = n-m-1.$$

Comme $\theta > 0$ et $1-\theta > 0$, les valeurs α et β sont prises, donc $1 \leq m \leq n-1$. Si $m=1$, on obtiendrait $n=2$, ce qui contredit $n \geq 3$; donc $m \geq 2$ et $\alpha^2 = \frac{n-m-1}{m-1}$. Ce réel est strictement positif, donc $n-m-1 > 0$, i.e. $m \leq n-2$, et alors $n \geq m+2 \geq 4$. Enfin

$$\theta = \frac{1}{1+\alpha^2} = \frac{m-1}{(m-1) + (n-m-1)} = \frac{m-1}{n-2}.$$

$$(A1) \quad \alpha_i = \sqrt{\frac{n-m_i-1}{m_i-1}}, \quad \theta_i = \frac{m_i-1}{n-2}; \quad (A2) \quad n \geq 4; \quad (A3) \quad 2 \leq m_i \leq n-2.$$

f) Cas équiprobable.

i) Si $p_k = 1/n$ pour tout k , alors $\theta_i = \mathbb{P}(X_i = \alpha_i) = m_i/n$. Avec (A1) : $\frac{m_i}{n} = \frac{m_i-1}{n-2}$, donc $m_i(n-2) = n(m_i-1)$, soit $n = 2m_i$.

$$n \text{ est pair}, \quad m_i = \frac{n}{2}, \quad \theta_i = \frac{1}{2}.$$

ii) Alors $\alpha_i = \sqrt{\frac{1-1/2}{1/2}} = 1$ et $\beta_i = -1$: tous les coefficients de M valent ± 1 (la dernière ligne vaut 1). De plus $D = \frac{1}{\sqrt{n}} I_n$ et $MD = \frac{1}{\sqrt{n}} M \in \mathcal{O}_n$ (22.c), donc ${}^t M M = n I_n$. La question 2 donne

$$M \text{ est une matrice de Hadamard.}$$

Partie III – Deux propriétés des matrices de Hadamard

Partie III – Extrema de F sur le groupe orthogonal

$F(A) = \sum_{i,j} |A_{i,j}|$, $S(A)_{i,j} = \text{sgn}(A_{i,j})$, $\langle A; B \rangle = \sum_{i,j} A_{i,j} B_{i,j}$, $\|A\| = \sqrt{\langle A; A \rangle}$, et $\varphi(x) = [x_{(i-1)n+j}]_{i,j}$. Ici $n \geq 3$. Questions 23 à 35.

Corrigé – Partie III.

23. L'application φ .

Chaque coefficient de $\varphi(x)$ est une coordonnée de x , donc $\varphi(\lambda x + \mu y) = \lambda \varphi(x) + \mu \varphi(y)$: φ est linéaire. L'application $(i, j) \mapsto (i-1)n+j$ est une bijection de $\llbracket 1; n \rrbracket^2$ sur $\llbracket 1; n^2 \rrbracket$ (division euclidienne de $k-1$ par n). Donc

$$\|\varphi(x)\|^2 = \sum_{i=1}^n \sum_{j=1}^n x_{(i-1)n+j}^2 = \sum_{k=1}^{n^2} x_k^2 = \|x\|^2.$$

$$\varphi \text{ est linéaire (et bijective) et } \|\varphi(x)\| = \|x\|.$$

24. Norme et trace.

$({}^tAA)_{j,j} = \sum_{i=1}^n A_{i,j}^2$, donc

$$\text{Tr}({}^tAA) = \sum_{j=1}^n \sum_{i=1}^n A_{i,j}^2 = \|A\|^2.$$

25. Encadrement de F .

Minoration. Pour une ligne i fixée,

$$\left(\sum_{j=1}^n |A_{i,j}| \right)^2 = \sum_{j=1}^n A_{i,j}^2 + \sum_{j \neq k} |A_{i,j}| |A_{i,k}| \geq \sum_{j=1}^n A_{i,j}^2,$$

donc $(\sum_j A_{i,j}^2)^{1/2} \leq \sum_j |A_{i,j}|$. On somme sur i .

Majoration. L'inégalité de Cauchy-Schwarz dans $\mathbb{R}^{n^2}$ appliquée aux familles $(1)_{i,j}$ et $(|A_{i,j}|)_{i,j}$ donne

$$F(A) = \sum_{i,j} 1 \cdot |A_{i,j}| \leq \left(\sum_{i,j} 1 \right)^{1/2} \left(\sum_{i,j} A_{i,j}^2 \right)^{1/2} = n \|A\|.$$

$$\sum_{i=1}^n \left(\sum_{j=1}^n A_{i,j}^2 \right)^{1/2} \leq F(A) \leq n \left(\sum_{i,j} A_{i,j}^2 \right)^{1/2}.$$

26. $\mathcal{K}_n$ est un fermé borné.

Fermé. Pour (i, j) fixé, $g_{i,j} : x \mapsto ({}^t\varphi(x)\varphi(x))_{i,j} = \sum_{k=1}^n x_{(k-1)n+i} x_{(k-1)n+j}$ est polynomiale en les coordonnées, donc continue sur $\mathbb{R}^{n^2}$. Or

$$\mathcal{K}_n = \bigcap_{(i,j)} g_{i,j}^{-1}(\{\delta_{i,j}\}),$$

intersection d'images réciproques de fermés par des fonctions continues : c'est un fermé.

Borné. Si $x \in \mathcal{K}_n$, $Q = \varphi(x) \in \mathcal{O}_n$ et, par les questions 23 et 24, $\|x\|^2 = \|Q\|^2 = \text{Tr}({}^tQQ) = \text{Tr}(I_n) = n$.

$$\boxed{\mathcal{K}_n \text{ est fermé et borné (inclus dans la sphère de rayon } \sqrt{n}).}$$

27. Contrôle des variations de $F \circ \varphi$.

Par l'inégalité triangulaire $||a| - |b|| \leq |a - b|$, puis la question 25 et la linéarité de φ :

$$|F(\varphi(x)) - F(\varphi(y))| \leq \sum_{i,j} |\varphi(x)_{i,j} - \varphi(y)_{i,j}| = F(\varphi(x - y)) \leq n\|\varphi(x - y)\| = n\|x - y\|.$$

$$\boxed{|F(\varphi(x)) - F(\varphi(y))| \leq n\|x - y\|.$$

28. Existence des extrema.

Posons $G = F \circ \varphi$. Pour x fixé, la question 27 et le théorème d'encadrement donnent $G(y) \rightarrow G(x)$ quand $y \rightarrow x$: G est continue sur $\mathbb{R}^{n^2}$. L'ensemble $\mathcal{K}_n$ est fermé borné (question 26) et non vide ($\varphi^{-1}(I_n) \in \mathcal{K}_n$). Par le théorème des bornes atteintes, G admet un minimum et un maximum sur $\mathcal{K}_n$. Comme φ réalise une bijection de $\mathcal{K}_n$ sur $\mathcal{O}_n$,

$$\boxed{F \text{ admet sur } \mathcal{O}_n \text{ un minimum } M_n^- \text{ et un maximum } M_n^+, \text{ atteints.}}$$

29. Valeur de M_n^- .

Soit $Q \in \mathcal{O}_n$. Comme ${}^tQQ = I_n$, Q est inversible d'inverse ${}^tQ$, donc $Q{}^tQ = I_n$: chaque ligne vérifie $\sum_j Q_{i,j}^2 = 1$. La minoration (1) donne $F(Q) \geq \sum_{i=1}^n 1 = n$. De plus $I_n \in \mathcal{O}_n$ et $F(I_n) = n$.

$$\boxed{M_n^- = n.}$$

30. Matrices réalisant le minimum.

Soit $Q \in \mathcal{O}_n$ telle que $F(Q) = n$. On a $F(Q) = \sum_i \sum_j |Q_{i,j}|$ avec, pour chaque i , $\sum_j |Q_{i,j}| \geq 1$ (question 25) ; la somme valant n , chaque inégalité est une égalité. D'après le calcul de la question 25, cela impose $\sum_{j \neq k} |Q_{i,j}| |Q_{i,k}| = 0$: chaque ligne a au plus un coefficient non nul, et exactement un, valant ± 1 , car la ligne est de norme 1. Chaque colonne est aussi de norme 1 (${}^tQQ = I_n$), donc contient au moins un coefficient non nul ; il y a n coefficients non nuls au total pour n colonnes, donc exactement un par colonne. Notons $\tau(i)$ la colonne du coefficient non nul de la ligne i et $\varepsilon_i \in \{-1, 1\}$ sa valeur : τ est bijective et, avec $\sigma = \tau^{-1}$,

$$Q_{i,j} = \varepsilon_i \delta_{j,\tau(i)} = \varepsilon_i \delta_{i,\sigma(j)}, \quad \text{i.e.} \quad Q = DP,$$

avec $D = \text{diag}(\varepsilon_1, \dots, \varepsilon_n)$ et P la matrice de permutation associée à σ . Réciproquement, une telle matrice est orthogonale (produit de deux matrices orthogonales, questions 1 et 4) et possède exactement n coefficients égaux à ± 1 , les autres nuls, donc $F(DP) = n$.

$$\boxed{F(Q) = n \iff Q = DP, \text{ } D \text{ diagonale à coefficients } \pm 1, \text{ } P \text{ de permutation.}}$$

Il y a $2^n n!$ telles matrices.

31. Expression de $F(Q)$.

Pour tout réel x , $x \operatorname{sgn}(x) = |x|$ (y compris pour $x = 0$), donc $\langle Q; S(Q) \rangle = F(Q)$. De plus $\|Q\|^2 = \operatorname{Tr}({}^tQQ) = n$ et $\|S(Q)\|^2 = n^2$ (coefficients ± 1). Ainsi

$$\left\| Q - \frac{1}{\sqrt{n}} S(Q) \right\|^2 = \|Q\|^2 - \frac{2}{\sqrt{n}} \langle Q; S(Q) \rangle + \frac{1}{n} \|S(Q)\|^2 = 2n - \frac{2}{\sqrt{n}} F(Q).$$

En multipliant par $\frac{\sqrt{n}}{2}$:

$$F(Q) = n\sqrt{n} - \frac{\sqrt{n}}{2} \left\| Q - \frac{1}{\sqrt{n}} S(Q) \right\|^2.$$

32. Majoration de M_n^+ et cas d'égalité.

Par la question 31, $F(Q) \leq n\sqrt{n}$ pour toute $Q \in \mathcal{O}_n$, donc $M_n^+ \leq n\sqrt{n}$.

- Si $M_n^+ = n\sqrt{n}$, le maximum étant atteint (question 28), il existe $Q \in \mathcal{O}_n$ avec $\|Q - \frac{1}{\sqrt{n}} S(Q)\| = 0$, soit $S(Q) = \sqrt{n} Q$. Alors $S(Q)$ a ses coefficients dans $\{-1, 1\}$ et ${}^tS(Q)S(Q) = n {}^tQQ = nI_n$: $S(Q)$ est de Hadamard (question 2).
- Si $H \in \mathcal{M}_n(\mathbb{R})$ est de Hadamard, $Q = \frac{1}{\sqrt{n}} H$ vérifie ${}^tQQ = \frac{1}{n} {}^tHH = I_n$, donc $Q \in \mathcal{O}_n$, et $F(Q) = n^2 \cdot \frac{1}{\sqrt{n}} = n\sqrt{n}$. Donc $M_n^+ \geq n\sqrt{n}$.

$$M_n^+ \leq n\sqrt{n}, \quad \text{avec égalité} \iff \text{il existe une matrice de Hadamard dans } \mathcal{M}_n(\mathbb{R}).$$

33. Cas où $4 \nmid n$.

D'après la partie I (question 8), s'il existe une matrice de Hadamard de taille $n \geq 2$, alors $n = 2$ ou $4 \mid n$. Ici $n \geq 3$ et $4 \nmid n$, donc il n'en existe pas, et la question 32 donne

$$M_n^+ < n\sqrt{n}.$$

34. Le cas $n = 3$.

Les colonnes de $U = U(\alpha, \beta)$ sont $u_1 = (\alpha, \beta, -\beta)$, $u_2 = (\beta, \alpha, \beta)$, $u_3 = (\beta, -\beta, -\alpha)$. On calcule

$$\begin{aligned} \|u_1\|^2 &= \|u_2\|^2 = \|u_3\|^2 = \alpha^2 + 2\beta^2, \\ {}^tu_1u_2 &= \alpha\beta + \alpha\beta - \beta^2 = \beta(2\alpha - \beta), \\ {}^tu_1u_3 &= \alpha\beta - \beta^2 + \alpha\beta = \beta(2\alpha - \beta), \\ {}^tu_2u_3 &= \beta^2 - \alpha\beta - \alpha\beta = -\beta(2\alpha - \beta). \end{aligned}$$

Ainsi $U \in \mathcal{O}_3 \iff \alpha^2 + 2\beta^2 = 1$ et $\beta(2\alpha - \beta) = 0$.

- Si $\beta = 0$: $\alpha^2 = 1$, d'où $(\alpha, \beta) = (\pm 1, 0)$.
- Si $\beta = 2\alpha$: $9\alpha^2 = 1$, d'où $(\alpha, \beta) = (\frac{1}{3}, \frac{2}{3})$ ou $(-\frac{1}{3}, -\frac{2}{3})$.

$$(\alpha, \beta) \in \left\{ (1, 0), (-1, 0), \left(\frac{1}{3}, \frac{2}{3}\right), \left(-\frac{1}{3}, -\frac{2}{3}\right) \right\}.$$

Comme U contient trois coefficients $\pm\alpha$ et six coefficients $\pm\beta$, $F(U) = 3|\alpha| + 6|\beta|$: on obtient $F = 3$ pour $(\pm 1, 0)$ et $F = 1 + 4 = 5$ pour $\pm(\frac{1}{3}, \frac{2}{3})$. Donc $M_3^+ \geq 5$. Comme 3 n'est pas multiple de 4, la question 33 donne $M_3^+ < 3\sqrt{3}$.

$$5 \leq M_3^+ < 3\sqrt{3} \simeq 5,196.$$

35. Le cas n pair.

- a) Chaque produit $x_i y_i$ vaut ± 1 . Si a est le nombre de produits égaux à 1, $\langle x; y \rangle = a - (n - a) = 2a - n$, entier pair puisque n est pair. Un entier pair non nul est de valeur absolue au moins 2 :

$$|\langle x; y \rangle| \geq 2.$$

- b) On écrit $\langle x; y \rangle - \langle u; v \rangle = \langle x - u; y \rangle + \langle u; y - v \rangle$. L'inégalité triangulaire et l'inégalité de Cauchy-Schwarz donnent

$$|\langle x; y \rangle - \langle u; v \rangle| \leq \|y\| \|x - u\| + \|u\| \|y - v\|.$$

Enfin, pour $a, b \geq 0$, $(a + b)^2 \leq 2(a^2 + b^2)$ (car $2ab \leq a^2 + b^2$), donc $a + b \leq \sqrt{2}(a^2 + b^2)^{1/2}$:

$$|\langle x; y \rangle - \langle u; v \rangle| \leq \sqrt{2}(\|y\|^2 \|x - u\|^2 + \|u\|^2 \|y - v\|^2)^{1/2}.$$

- c) Les coefficients de $S = S(Q)$ valent ± 1 ; comme S n'est pas de Hadamard, deux de ses colonnes s_j, s_k ($j \neq k$) ne sont pas orthogonales, donc $|\langle s_j; s_k \rangle| \geq 2$ par a). Notons q_j, q_k les colonnes correspondantes de Q : $\langle q_j; q_k \rangle = 0$ et $\|q_j\| = \|q_k\| = 1$. On applique b) avec $x = q_j$, $y = q_k$, $u = \frac{1}{\sqrt{n}} s_j$, $v = \frac{1}{\sqrt{n}} s_k$, où $\|u\| = 1$:

$$\begin{aligned} \frac{2}{n} &\leq \frac{1}{n} |\langle s_j; s_k \rangle| = |\langle q_j; q_k \rangle - \langle u; v \rangle| \\ &\leq \sqrt{2} \left(\|q_j - \frac{s_j}{\sqrt{n}}\|^2 + \|q_k - \frac{s_k}{\sqrt{n}}\|^2 \right)^{1/2} \\ &\leq \sqrt{2} \left\| Q - \frac{1}{\sqrt{n}} S \right\|, \end{aligned}$$

la dernière inégalité venant de ce que $\|Q - \frac{1}{\sqrt{n}} S\|^2$ est la somme des carrés des normes de toutes les colonnes de $Q - \frac{1}{\sqrt{n}} S$. On en déduit $\|Q - \frac{1}{\sqrt{n}} S\| \geq \frac{\sqrt{2}}{n}$, soit

$$\left\| Q - \frac{1}{\sqrt{n}} S(Q) \right\|^2 \geq \frac{2}{n^2}.$$

- d) S'il n'existe aucune matrice de Hadamard dans $\mathcal{M}_n(\mathbb{R})$, alors pour toute $Q \in \mathcal{O}_n$, $S(Q)$ n'est pas de Hadamard ; les questions 31 et c) donnent

$$F(Q) \leq n\sqrt{n} - \frac{\sqrt{n}}{2} \cdot \frac{2}{n^2} = n\sqrt{n} - \frac{\sqrt{n}}{n^2} = n\sqrt{n} - \frac{1}{n\sqrt{n}}.$$

Le maximum étant atteint en un élément de $\mathcal{O}_n$,

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