Centrale/Supélec Matrices carrées à
Année 2016 coefficients 0 ou 1
Épreuve 1

Dans tout ce problème, n est un entier supérieur ou égal à 2 et l'on note :
- $\mathfrak{M}_n(\mathbb{R})$ l'ensemble des matrices carrées d'ordre n à coefficients réels ;
- $\mathrm{GL}_n(\mathbb{R})$ l'ensemble des éléments inversibles de $\mathfrak{M}_n(\mathbb{R})$;
- $O_n(\mathbb{R})$ l'ensemble des matrices orthogonales d'ordre n ;
- $\mathcal{X}_n$ l'ensemble des éléments de $\mathfrak{M}_n(\mathbb{R})$ dont tous les coefficients sont dans $\{0,1\}$;
- $\mathcal{Y}_n$ l'ensemble des éléments de $\mathfrak{M}_n(\mathbb{R})$ dont tous les coefficients sont dans $[0,1]$;
- $\mathcal{P}_n$ l'ensemble des éléments de $\mathfrak{M}_n(\mathbb{R})$ dont tous les coefficients sont dans $\{0,1\}$ et ne contenant qu'un seul coefficient non nul par ligne et par colonne ;
- ${}^tM$ la transposée d'une matrice M, mais la notation M^T est également utilisable.

Par exemple :

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathcal{X}_3 \qquad \begin{pmatrix} \dfrac{1}{\sqrt{2}} & 0 \\ \exp(-1) & \dfrac{3}{4} \end{pmatrix} \in \mathcal{Y}_2 \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{P}_3$$

Ce problème aborde l'étude de matrices à coefficients dans $\{0,1\}$ à travers plusieurs thématiques indépendantes les unes des autres. Les deux premières parties étudient quelques propriétés algébriques et topologiques des ensembles $\mathcal{X}_n$ et $\mathcal{Y}_n$ définis ci-dessus. La partie III étudie le cas particulier des matrices de permutation. La partie IV étudie deux modalités de génération aléatoire de matrices à coefficients dans $\{0,1\}$·

I Généralités

I.A – Propriétés élémentaires

I.A.1) Justifier que $\mathcal{X}_n$ est un ensemble fini et déterminer son cardinal.

I.A.2) Démontrer que pour tout $M \in \mathcal{Y}_n$, $\det(M) \leqslant n!$ et qu'il n'y a pas égalité.

I.A.3) Démontrer que $\mathcal{Y}_n$ est une partie convexe et compacte de $\mathfrak{M}_n(\mathbb{R})$.

I.A.4) Soit $M \in \mathcal{Y}_n$ et λ une valeur propre complexe de M. Démontrer que $|\lambda| \leqslant n$ et donner un exemple explicite où l'on a l'égalité.

I.B – Étude de $\mathcal{X}'_n = \mathcal{X}_n \cap \mathrm{GL}_n(\mathbb{R})$.

I.B.1) Faire la liste des éléments de $\mathcal{X}'_2$. Préciser (en justifiant) ceux qui sont diagonalisables sur $\mathbb{R}$.

I.B.2) Démontrer que $\mathcal{X}'_2$ engendre l'espace vectoriel $\mathfrak{M}_2(\mathbb{R})$. Est-ce que, pour $n \geqslant 2$, $\mathcal{X}'_n$ engendre l'espace vectoriel $\mathfrak{M}_n(\mathbb{R})$?

II Deux problèmes d'optimisation

II.A – Étude de la distance à $\mathcal{Y}_n$

Pour tout $(M, N) \in \big(\mathfrak{M}_n(\mathbb{R})\big)^2$, on note $\big(M|N\big) = \mathrm{tr}({}^tMN)$.

II.A.1) Démontrer que l'on définit ainsi un produit scalaire sur $\mathfrak{M}_n(\mathbb{R})$.
Expliciter $\big(M|N\big)$ en fonction des coefficients de M et N.
On notera $\|M\|$ la norme euclidienne associée.

II.A.2) On fixe $A \in \mathfrak{M}_n(\mathbb{R})$, prouver qu'il existe une matrice $M \in \mathcal{Y}_n$ telle que : $\forall N \in \mathcal{Y}_n,\ \|A - M\| \leqslant \|A - N\|$.

II.A.3) Justifier l'unicité de la matrice M ci-dessus et expliciter ses coefficients en fonction de ceux de A.

II.B – Maximisation du déterminant sur $\mathcal{X}_n$ et $\mathcal{Y}_n$

II.B.1) Justifier que le déterminant possède un maximum sur $\mathcal{X}_n$ (noté x_n) et un maximum sur $\mathcal{Y}_n$ (noté y_n).

II.B.2) Démontrer que la suite $(y_k)_{k\geqslant 2}$ est croissante.

II.B.3) Soit $J \in \mathcal{X}_n$ la matrice dont tous les coefficients valent 1. On pose $M = J - I_n$.
Calculer $\det(M)$ et en déduire que $\displaystyle\lim_{k\to+\infty} y_k = +\infty$.

II.B.4) Soit $N = \big(n_{i,j}\big)_{i,j} \in \mathcal{Y}_n$. Fixons $1 \leqslant i, j \leqslant n$ et supposons que $n_{i,j} \in]0, 1[$.
Démontrer qu'en remplaçant $n_{i,j}$ soit par 0, soit par 1, on peut obtenir une matrice N' de $\mathcal{Y}_n$ telle que $\det(N) \leqslant \det(N')$.
En déduire que $x_n = y_n$.

III Matrices de permutations

On munit $\mathbb{R}^n$ de sa structure euclidienne canonique et $(e_1, \ldots, e_n)$ désigne sa base canonique.
On note S_n l'ensemble des bijections de l'ensemble $\{1, \ldots, n\}$ dans lui-même (appelées permutations).

Pour tout $\sigma \in S_n$, on note P_σ la matrice de $\mathcal{P}_n$ dont le coefficient ligne i, colonne j vaut 1 si $i = \sigma(j)$ et 0 sinon.
On dit que P_σ est la matrice de permutation associée à σ.
On note u_σ l'endomorphisme de $\mathbb{R}^n$ canoniquement associé à P_σ.

III.A – Description de $\mathcal{P}_n$

III.A.1) Donner deux définitions d'une isométrie vectorielle de $\mathbb{R}^n$ et démontrer leur équivalence.

III.A.2) Démontrer que si $M \in O_n(\mathbb{R})$, alors son déterminant vaut 1 ou -1. Que penser de la réciproque ?

III.A.3) Démontrer que $\mathcal{P}_n = \mathcal{X}_n \cap O_n(\mathbb{R})$ et déterminer son cardinal.

III.B – Quelques propriétés des éléments de $\mathcal{P}_n$

III.B.1) Soient σ et σ' deux éléments de S_n.
Démontrer que $P_\sigma P_{\sigma'} = P_{\sigma \circ \sigma'}$.
Justifier que l'application $\begin{pmatrix} \mathbb{Z} & \to & S_n \\ k & \mapsto & \sigma^k \end{pmatrix}$ n'est pas injective.
En déduire qu'il existe un entier $N \geqslant 1$ tel que $\sigma^N = Id_{\{1,\ldots,n\}}$, où $Id_{\{1,\ldots,n\}}$ désigne l'application identité sur l'ensemble $\{1, \ldots, n\}$.

III.B.2) Démontrer que tous les éléments de $\mathcal{P}_n$ sont diagonalisables sur $\mathbb{C}$.

III.B.3) Déterminer les vecteurs propres communs à tous les éléments de $\mathcal{P}_n$ dans les cas $n = 2$ et $n = 3$.

III.B.4) On se propose de démontrer que les seuls sous-espaces vectoriels de $\mathbb{R}^n$ stables par tous les u_σ, $\sigma \in S_n$ sont $\{0_{\mathbb{R}^n}\}$, $\mathbb{R}^n$, la droite D engendrée par $e_1 + e_2 + \cdots + e_n$ et l'hyperplan H orthogonal à D.

a) Vérifier que ces quatre sous-espaces vectoriels sont stables par tous les u_σ.

b) Soit V un sous-espace vectoriel de $\mathbb{R}^n$, non contenu dans D et stable par tous les u_σ. Démontrer qu'il existe un couple $(i, j) \in \{1, \ldots, n\}^2$ avec $i \neq j$ tel que $e_i - e_j \in V$, puis que les $n - 1$ vecteurs $e_k - e_j$ $(k \in \{1, \ldots, n\},\ k \neq j)$ appartiennent à V.

c) Conclure.

III.C – Une caractérisation des éléments de $\mathcal{P}_n$

On se donne une matrice M de $\mathrm{GL}_n(\mathbb{R})$ dont tous les coefficients sont des entiers naturels et telle que l'ensemble formé par tous les coefficients de toutes les puissances successives de M est fini.
Démontrer que M^{-1} est à coefficients dans $\mathbb{N}$ et en déduire que M est une matrice de permutation. Que dire de la réciproque ?

IV Matrices aléatoires de $\mathcal{X}_n$

IV.A – Génération par une colonne aléatoire

Soit $p \in]0,1[$. Soient $X_1, \ldots, X_n$ des variables aléatoires mutuellement indépendantes, définies sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ et suivant une même loi de Bernoulli de paramètre p.

IV.A.1) Calculer la probabilité que $X_1, \ldots, X_n$ soient égales.

IV.A.2) Quelle est la loi de $S = X_1 + \cdots + X_n$? On attend une démonstration du résultat annoncé.

IV.A.3) Soient i et j dans $\{1, \ldots, n\}$· Donner la loi de la variable aléatoire $X_{i,j} = X_i \times X_j$.

IV.A.4) Si $\omega \in \Omega$, on introduit la matrice colonne $U(\omega) = \begin{pmatrix} X_1(\omega) \\ \vdots \\ X_n(\omega) \end{pmatrix}$

et la matrice $M(\omega) = U(\omega)\,{}^tU(\omega)$.

L'application $M : \begin{pmatrix} \Omega & \to & \mathfrak{M}_n(\mathbb{R}) \\ \omega & \mapsto & M(\omega) \end{pmatrix}$ est ainsi une variable aléatoire.

a) Si $\omega \in \Omega$, justifier que $M(\omega) \in \mathcal{X}_n$.

b) Si $\omega \in \Omega$, justifier que $\operatorname{tr}\big(M(\omega)\big) \in \{0, \ldots, n\}$, que $M(\omega)$ est diagonalisable sur $\mathbb{R}$ et que $\operatorname{rg}\big(M(\omega)\big) \leqslant 1$.

c) Si $\omega \in \Omega$, justifier que $M(\omega)$ est une matrice de projection orthogonale si et seulement si $S(\omega) \in \{0, 1\}$·

IV.A.5) Donner la loi, l'espérance et la variance des variables aléatoires $\operatorname{tr}(M)$ et $\operatorname{rg}(M)$.

IV.A.6) Exprimer M^k en fonction de S et M.
Quelle est la probabilité pour que la suite de matrices $(M^k)_{k \in \mathbb{N}}$ soit convergente ?
Montrer que, dans ce cas, la limite est une matrice de projection.

IV.A.7) Quelle est la probabilité que M admette deux valeurs propres distinctes ?

IV.B – Génération par remplissage aléatoire

Soit $p \in]0,1[$. On part de la matrice nulle de $\mathfrak{M}_n(\mathbb{R})$, notée M_0. Pour tout $k \in \mathbb{N}$, on construit la matrice M_{k+1} à partir de la matrice M_k de la manière suivante
- on parcourt en une vague la matrice et chaque coefficient nul est changé en 1 avec la probabilité p ;
- chaque action sur un coefficient est indépendante de ce qui se passe sur les autres et des vagues précédentes.

Les M_k sont donc des variables aléatoires à valeurs dans $\mathcal{X}_n$ et l'on considère qu'elles sont définies sur un espace probabilisé commun $(\Omega, \mathcal{A}, \mathbb{P})$.
Voici un exemple de réalisation de cette évolution pour $n = 2$

$$M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \to M_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \to M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \to M_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M_3 \to M_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \to M_5 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Pour $k \geqslant 1$, le nombre de modifications réalisées lors de la k-ième vague est noté N_k. Dans l'exemple ci-dessus :
$N_1 = 2,\ N_2 = 0,\ N_3 = 1,\ N_4 = 1,\ N_5 = 0.$
On s'intéresse au plus petit indice k pour lequel la matrice M_k ne comporte que des 1 ; on dit alors qu'elle est totalement remplie. Dans l'exemple précédent, ce premier indice vaut 4.
On note $q = 1 - p$ et $m = n^2$.

IV.B.1) Dans toute cette question on utilise le langage Python. M désigne une matrice carrée d'ordre n. Ses lignes et ses colonnes sont numérotées de 0 à $n - 1$. L'expression `M[i,j]` permet d'accéder à l'élément situé à l'intersection de la ligne i et de la colonne j et `len(M)` donne l'ordre de la matrice M.

a) Écrire une fonction `Somme(M)` qui renvoie la somme des coefficients de la matrice M.

b) Écrire une fonction `Bernoulli(p)` qui renvoie 1 avec la probabilité p et 0 avec la probabilité $1 - p$. On pourra utiliser l'expression `random()` qui renvoie un réel de l'intervalle $[0, 1[$ selon la loi uniforme.

c) À l'aide de la fonction `Bernoulli(p)`, écrire une fonction `Modifie(M,p)` qui modifie aléatoirement la matrice M suivant le principe décrit au IV.B ci-dessus.

d) Écrire une fonction `Simulation(n,p)` qui renvoie le plus petit entier k tel que M_k est totalement remplie à partir d'un remplissage aléatoire de la matrice nulle d'ordre n (qui peut être obtenue par `zeros((n,n))`). Il n'est pas demandé de mémoriser les M_k.

IV.B.2) Donner la loi de N_1, puis la loi conditionnelle de N_2 sachant $(N_1 = i)$ pour i dans un ensemble à préciser. N_1 et N_2 sont-elles indépendantes ?

IV.B.3) Soient i et j dans $\{1, \ldots, n\}\cdot$ Le plus petit entier $k \geqslant 1$ tel que le coefficient ligne i, colonne j de M_k vaut 1 est noté $T_{i,j}$ (dans l'exemple ci-dessus : $T_{1,1} = 1$ et $T_{1,2} = 3$). Donner la loi de $T_{i,j}$.

IV.B.4) Pour un entier $k \geqslant 1$, donner la valeur de $P(T_{i,j} \geqslant k)$.

IV.B.5) Soient $r \geqslant 1$ un entier et $S_r = N_1 + \cdots + N_r$. Que représente S_r ? Donner sa loi (on pourra utiliser la question précédente).

IV.B.6) On note N le plus petit indice k pour lequel la matrice M_k est totalement remplie.

a) Proposer une démarche pour approcher l'espérance de N à l'aide d'une simulation informatique utilisant les fonctions précédentes.

b) Donner une expression de la valeur exacte de cette espérance faisant intervenir q et m.

Solution

I Généralités

I.A -

I.A.1) $\mathcal{X}_n$ est en bijection avec $\{0,1\}^{n^2}$ et, donc, $\mathrm{Card}(\mathcal{X}_n) = 2^{(n^2)}$.

I.A.2) On procède par récurrence.
Si $(a,b,c,d) \in [0,1]^4$ alors $ad - bc \leqslant ad \leqslant 1 < 2!$.
Si, pour un entier $n \geqslant 2$, les déterminants des éléments de $\mathcal{Y}_n$ sont strictement inférieurs à $n!$ et si $M \in \mathcal{Y}_{n+1}$, alors le développement selon la première colonne fournit, avec des notations classiques :
$\det(M) = \sum\limits_{i=1}^{n+1} m_{i,1}\Delta_{i,1} \leqslant \left(\max\limits_{1\leqslant i\leqslant n+1} \Delta_{i,1}\right) \sum\limits_{i=1}^{n+1} m_{i,1} < n! \sum\limits_{i=1}^{n+1} m_{i,1} < (n+1)!$
car, par hypothèse de récurrence, $\forall i \in [\![1, n+1]\!]$, $\Delta_{i,k} < n!$ (ce sont des déterminants d'éléments de $\mathcal{Y}_n$) et $0 \leqslant \sum\limits_{i=1}^{n+1} m_{i,1} \leqslant n+1$.
Le théorème de récurrence montre que $\det < n!$ sur $\mathcal{Y}_n$ pour tout n.

I.A.3) Les coefficients de tout élément de $\mathcal{Y}_n$ étant bornés, $\mathcal{Y}_n$ est une partie bornée de $\mathfrak{M}_n(\mathbb{R})$.
Si $(M^{(p)})_p$ est une suite convergente d'éléments de $\mathcal{Y}_n$, de limite notée M alors $\forall (i,j) \in [\![1,n]\!]^2$, $m_{i,j}^{(p)} \xrightarrow[p\to\infty]{} m_{i,j} \in [0,1]$ partie fermée de $\mathbb{R}$, et donc $\mathcal{Y}_n$ est fermée dans $\mathfrak{M}_n(\mathbb{R})$.
Enfin si $(M,N,t) \in (\mathcal{Y}_n)^2 \times [0,1]$, $\forall (i,j) \in [\![1,n]\!]^2$, $0 \leqslant tm_{i,j} + (1-t)n_{i,j} \leqslant 1$, d'où $tM + (1-t)N \in \mathcal{Y}_n$ et Y_n est une partie à la fois compacte et convexe de $\mathfrak{M}_n(\mathbb{R})$. Elle est de plus non vide car elle contient 0_n par exemple.

I.A.4) Si X est un vecteur propre de M associé à λ et si i est un élément de $[\![1,n]\!]$ tel que $|x_i|$ est maximal alors
$MX = \lambda X \Rightarrow |\lambda x_i| = \left|\sum\limits_{k=1}^{n} m_{i,k}x_k\right| \leqslant \sum\limits_{k=1}^{n} m_{i,k}|x_k| \leqslant |x_i| \sum\limits_{k=1}^{n} m_{i,k} \leqslant n|x_i|$
d'où, comme $|x_i| > 0$, $|\lambda| \leqslant n$.
Si $\forall (i,j) \in [\![1,n]\!]^2$, $m_{i,j} = 1$, alors $M \in \mathcal{Y}_n$ et $MU = nU$ si $U = {}^t(1 \cdots 1)$.

I.B -

I.B.1) Les éléments de $\mathcal{X}_2'$ sont
I_2 diagonale
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ diagonalisables car symétriques réelles,
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et sa transposée non diagonalisables car de caractéristique $(X-1)^2$ et car la seule matrice diagonalisable ayant ce caractéristique est I_2.

I.B.2) Si $i \neq j$ alors $I_n + E_{i,j} \in \mathcal{X}_n'$ et $E_{i,j} = (I_n + E_{i,j}) - I_n \in \mathrm{Vect}(X_n')$.
Remarquons que $\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{A} - \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}}_{B} + E_{2,1} = E_{1,1} \in \mathrm{Vect}(\mathcal{X}_2')$ et alors, par blocs, $E_{i,i} = \mathrm{Diag}(I_{i-1}, A, I_{n-i-1}) - \mathrm{Diag}(I_{i-1}, B, I_{n-i-1}) + E_{i+1,i} \in \mathrm{Vect}(\mathcal{X}_n')$ si $i < n$.
De même $E_{n,n} = \mathrm{Diag}(I_{n-2}, C) - \mathrm{Diag}(I_{n-2}, D) + E_{n-1,n} \in \mathrm{Vect}(\mathcal{X}_n')$ si l'on pose $C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et comme les $E_{i,j}$ forment une base de $\mathfrak{M}_n(\mathbb{R})$, on en déduit que, pour tout $n \geqslant 2$, $\mathfrak{M}_n(\mathbb{R}) = \mathrm{Vect}(\mathcal{X}_n')$.

II Deux problèmes d'optimisation

II.A -

II.A.1) $\big(M|N\big) = \sum\limits_{1 \leqslant i,j \leqslant n} m_{i,j} n_{i,j}$; ainsi $\big(\cdot|\cdot\big)$ est le produit scalaire canonique sur $\mathfrak{M}_n(\mathbb{R})$ identifié à $\mathbb{R}^{(n^2)}$.

II.A.2) et 3) $\forall M \in \mathcal{Y}_n,\ \|A - M\|^2 = \sum\limits_{1 \leqslant i,j \leqslant n} (a_{i,j} - m_{i,j})^2$ et donc la fonction $M \mapsto \|A - M\|$ est minimale sur $\mathcal{Y}_n$ en M si, et seulement si, $\forall (i,j) \in [\![1,n]\!]^2$, $m_{i,j} \mapsto |a_{i,j} - m_{i,j}|$ est minimale en $m_{i,j}$ *i.e.* $m_{i,j}$ est l'élément de $[0,1]$ le plus proche de $a_{i,j}$ dans $\mathbb{R}$.
Pour tout $(i,j) \in [\![1,n]\!]^2$ le problème de minimisation précédent a une et une seule solution : $m_{i,j} = \begin{cases} 0 & \text{si } a_{i,j} < 0 \\ a_{i,j} & \text{si } 0 \leqslant a_{i,j} \leqslant 1 \\ 1 & \text{sinon} \end{cases}$

II.B -

II.B.1) $\mathcal{X}_n$ est fini non vide d'où l'existence de $\max\big(\det(\mathcal{X}_n)\big)$.
det est continue car polynomiale en les coefficients des matrices et $\mathcal{Y}_n$ est une partie compacte et non vide de $\mathfrak{M}_n(\mathbb{R})$, d'où l'existence de $\max\big(\det(\mathcal{Y}_n)\big)$.

II.B.2) $M \in \mathcal{Y}_n \Rightarrow \mathrm{Diag}(1, M) \in \mathcal{Y}_{n+1}$ d'où $\det(Y_n) \subset \det(\mathcal{Y}_{n+1})$ et, donc, $y_n \leqslant y_{n+1}$.

II.B.3) On reprend la notation U de I.A.4 et on note c la base canonique $(E_1, \ldots, E_n)$ de $\mathfrak{M}_{n,1}(\mathbb{R})$.

$\det(-M) = \det_c(E_1 - U, \ldots, E_n - U) = \det_c(E_1, \ldots, E_n) - \sum\limits_{i=1}^{n} \Delta_i$ où Δ_i est le déterminant dans c de la famille obtenue en remplaçant, dans c, E_i par U.

Si $i > 1$, $\Delta_i = \begin{vmatrix} I_{i-1} & \star \\ 0 & A \end{vmatrix}$ par blocs où $A = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (\star) & & 1 \end{pmatrix}$ est de déterminant 1 donc $\Delta_i = 1$. Encore plus facilement $\Delta_1 = 1$ d'où

$$\det(M) = (-1)^n(1-n).$$

$-M \in \mathcal{Y}_n \Rightarrow y_n \geqslant n-1 \Rightarrow y_n \xrightarrow[n\to\infty]{} +\infty.$

II.B.4) En développant selon la i-ème ligne il vient $\det(N) = An_{i,j} + B$ où (A, B) est un couple de nombre réels indépendants de $n_{i,j}$.

En posant $n'_{i,j} = \begin{cases} 1 & \text{si } A \geqslant 0 \\ 0 & \text{sinon} \end{cases}$ alors $\det(N) \leqslant \det(N')$.

En effectuant successivement le procédé précédent quand (i, j) décrit $[\![1, n]\!]^2$ dans l'ordre lexicographique par exemple on met en évidence un élément N' de $\mathcal{X}_n$ tel que $\det(N) \leqslant \det(N') \leqslant x_n$, d'où $y_n \leqslant x_n$.

Comme, de plus, $\mathcal{X}_n \subset \mathcal{Y}_n$, cela montre $x_n = y_n$.

III Matrices de permutations

III.A -

III.A.1) Si $u \in \mathcal{L}(\mathbb{R}^n)$ on dit que u est une isométrie
si (1) $\quad \forall x \in \mathbb{R}^n,\ \big\|u(x)\big\| = \|x\|$
ou encore si (2) $\quad \forall (x, y) \in (\mathbb{R}^n)^2,\ \big(u(x)|u(y)\big) = \big(x|y\big)$.
Immédiatement (2) $\Rightarrow$ (1) et une identité de polarisation établit la réciproque.

III.A.2) $M \in O_n(\mathbb{R}) \Rightarrow {}^tMM = I_n \Rightarrow \det({}^tMM) = \det(I_n) \Rightarrow \det^2(M) = 1$ d'où $\det(M) \in \{-1, 1\}$·

Si $D = \mathrm{Diag}(2, 1/2, 1, \ldots, 1)$ alors $\det(D) = 1$ mais $D \notin O_n(\mathbb{R})$.

III.A.3) Soit $M \in \mathcal{P}_n$. L'application σ qui à tout j de $[\![1, n]\!]$ associe l'indice i de ligne tel que $m_{i,j} = 1$ est élément de S_n, donc $M = P_\sigma$.

Si l'on note encore $(E_1, \ldots, E_n)$ la base canonique de $\mathfrak{M}_{n,1}(\mathbb{R})$ alors la famille des colonnes de M est $(E_{\sigma(1)}, \ldots, E_{\sigma(n)})$ qui est une base orthonormale de $\mathbb{R}^n$, ainsi $M \in \mathcal{X}_n \cap O_n(\mathbb{R})$.

Réciproquement si $M \in \mathcal{X}_n \cap O_n(\mathbb{R})$ alors, comme chaque colonne est unitaire, dans chaque colonne il existe un et un seul coefficient non nul et il vaut 1. Il en va de même pour chaque ligne car ${}^tM \in \mathcal{X}(n) \cap O_n(\mathbb{R})$, donc $M \in \mathcal{P}_n$.

En fait $S_n \to \mathcal{P}_n,\ \sigma \mapsto P_\sigma$ est une bijection, d'où $\mathrm{Card}(\mathcal{P}_n) = n!$.

III.B -

III.B.1) Soit $M = P_\sigma P_{\sigma'}$.

$\forall (i, j) \in [\![1, n]\!]^2,\ m_{i,j} = \sum\limits_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{k,\sigma'(j)} = \delta_{i,\sigma(\sigma'(j))}$ car pour $k \neq \sigma'(j)$ le terme de la somme est nul. Cela montre $P_\sigma P_{\sigma'} = P_{\sigma\circ\sigma'}$.