W

Rapport de recherches bibliographiques

Les matrices de Hadamard

DE SOUSA Maxime

DE OLIVEIRA-MANGIN Lucas

Avec la très précieuse aide de Mr NECHITA Ion

UNIVERSITÉ TOULOUSE III PAUL SABATIER

Université de Toulouse

Table des matières

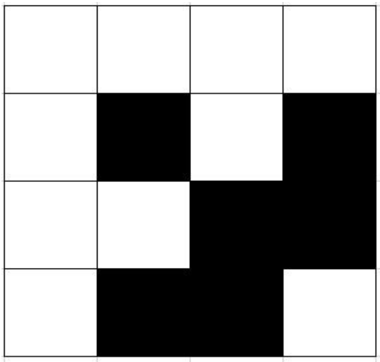
I – L'histoire des matrices d'Hadamard.

I.1 – La question initiale.

Comme beaucoup d'objets mathématiques, les matrices de Hadamard répondent à un problème très particulier. C'est grâce aux jeux d'échecs que en 1893 Jacques Salomon Hadamard, un mathématicien français du $XIX^{ème}$ et du $XX^{ème}$ siècles , trouva ces matrices qui portent sont nom.

Avant de comprendre le problème, il faut présenter la notion d'échiquier égalitaire.

Prenons un échiquier spécial de 4 lignes et 4 colonnes. Il faut maintenant colorier l'échiquier, à priori de manière aléatoire. Voici un des résultats possibles :



L'idée de Hadamard, c'est de s'amuser à compter les concordances de couleurs. Prenons par exemple les lignes 1 et 2 de l'échiquier. Nous pouvons compter 2 concordances de couleurs. De même , avec les lignes 2 et 4.

Définition :On dit alors qu'**un échiquier est égalitaire** si et seulement si il est de taille carré $n \times n$ et les nombre de concordances de couleurs est toujours égale à $\frac{n}{2}$ entre n'importe laquelle de deux de ces lignes.

Les questions majeures de cette énoncé découlent naturellement de cette définition ;

Pour quel n entier existe-t-il un échiquier égalitaire de taille $n \times n$?

Existe-t-il une infinité de n ? Si non, peut-on les déterminer ?

Pour la suite, les termes matrice égalitaire, matrice de Hadamard ou échiquier anallagmatique de Sylvester désignent le même objet mathématique.

I.2 – Échiquiers anallagmatique de Sylvester.

L'idée original de cette représentation en échiquier ne vient pas en fait de Hadamard, mais de James Joseph Sylvester, qui publie en 1867 un article qui traite des échiquiers égalitaires.

Il fournit la toute première construction systématique d'échiquiers égalitaires, d'ordre $n=2^p$, où p est un entier positif. L'idée se base sur la propriété, qui sera énoncer clairement plus tard, que le produit de Kroenecker d'une matrice de Hadamard par une autre matrice de Hadamard quelconque est égale à une matrice de Hadamard.

La vraie méthode est la suivante ; on note A une matrice de Hadamard d'ordre n et $\tilde{A}$ l'opposée de A . Alors on peut construire une matrice B de Hadamard tel que $B=\begin{pmatrix} A & A \\ A & \tilde{A} \end{pmatrix}$. De plus amples détails sur cette construction seront abordés dans la cinquième sous-partie.

I.3 – La conjecture de Hadamard.

Tout échiquier peut-être modélisé par un tableau, et donc par une matrice. Plaçons nous dans l'ensemble des matrices carrées de taille n , prenant pour valeurs $[-1,1]$,soit $M_n(\pm 1)$

Soit l'échiquier de l'introduction modélisé par la matrice suivante :

$$H_4=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Définition *:* On dit qu'**une matrice est de Hadamard** si le produit scalaire est nul entre n'importe lesquelles de ses lignes.

Cette définition traduit le caractère égalitaire de l'échiquier associé à la matrice. Elle est cependant pour le moment provisoire. Nous verrons par la suite que plusieurs autres propriétés peuvent êtres affirmés sur les matrices de Hadamard.

Un des premiers résultats qui nous permet des construire une réponse aux questions initiales est une condition nécessaire sur la multiplicité de n est le suivant :

Propriété:

$$\text{Soit } A\in M_n(\pm 1)\text{; } A \text{ est une matrice de Hadamard} \Rightarrow (n=1)\cup(n=2)\cup(n \text{ est multiple de } 4) \ .$$

Démonstration a.

En d'autre termes, si A est une matrice de Hadamard, alors la taille de A est au moins égale à 1, ou égale à 2, ou multiple de 4. Cette propriété permet cependant que, pour certain multiples de 4, il n'existe aucune matrice de Hadamard.

La conjecture de Hadamard consiste à dire que la condition *nécessaire* de multiplicité sur n est aussi une condition *suffisante.* La conjecture s'énonce de cette manière :

Conjecture :

$$\forall\ n\, multiples\, de\, 4\,,\exists\ A\in M_n(\pm 1)\, tel\, que\, A\, est\, une\, matrice\, de\, Hadamard$$

Définition **:** On appelle **nombre de Hadamard** tout entier n pour lequel il existe au moins une matrice de Hadamard de taille $n\times n$.

La démonstration de cette conjecture est le principal objectif de notre programme.

I.4 – Les avancées majeures après Hadamard.

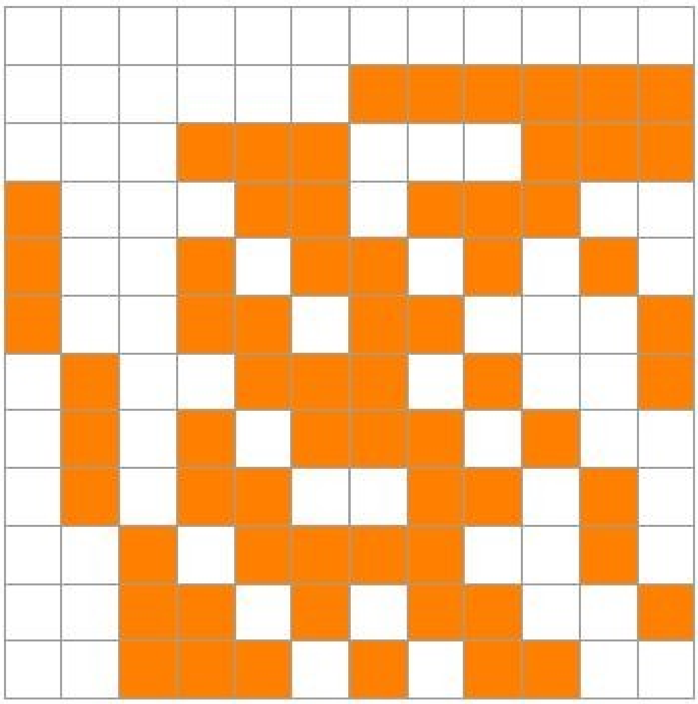
En 1898, Umberto Scarpis, mathématicien italien, énonce le théorème suivant :

Théorème : Soit n un multiple de 4 tel que $n-1$ soit un nombre premier. Si il existe une matrice de Hadamard d'ordre n , alors il en existe une plus grande d'ordre $(n-1)n$.

L'astuce de Scarpis est de recombiner les lignes et les colonnes de la matrice de taille n

Ce théorème permet la construction systématique de matrices de Hadamard, pour des nombres autres que les puissances de 2. Scarpis semble s'être d'ailleurs inspirer de la construction de Hadamard de la matrice de taille 12x12.

Voici cette matrice d'ordre 12 :



Ce théorème est encore compléter récemment, comme vu par exemple dans l'article [01], datant de 2016, présentant une généralisation du théorème pour les puissances de nombres premiers, en contournant la condition de Scarpis.

L'avancée majeure suivante est due à un duo de mathématiciens, Ray Edwin Gilman et Raymond Paley.

Tout d'abord, Gilman propose en 1930 un théorème qui s'énonce de cette façon :

Soit n un multiple de 4 tel que $n-1$ soit un nombre premier. Alors il existe une matrice de Hadamard d'ordre n .

On remarque que ce théorème est très similaire au théorème de Scarpis. C'est en fait parce que Gilman démontre ici que la condition d'existence d'une matrice de Hadamard pour l'ordre n est tout le temps vraie. Gilman fait ici un énorme progrès, puisque l'on pouvait dès lors prouver l'existence de nouveaux ordres de matrices de Hadamard.

Gilman, n'ayant publié aucun article sur sa démonstration en 1930, se fera en quelque sorte volé la vedette par un jeune mathématicien de 26 ans, Raymond Paley, qui publie en 1933 dans un article une version généralisée du théorème de Gilman.

Son théorème s'énonce de la manière suivante :

Théorème : Soit n un multiple de 4 tel que $n-1$ ou $\frac{n}{2}-1$ soit une puissance de nombre premier. Alors il existe une matrice de Hadamard d'ordre n .

Ce théorème est bien plus subtile, puisqu'il fait apparaître les puissances de nombres premiers ($\textit{Soit } q \textit{ premier et } a \textit{ entier}, a \geqslant 1, p = q^a \textit{ est une puissance de nombre premier}$.)

Grâce aux découvertes de Gilman et Paley, des 25 multiples de 4 compris entre 1 et 100, seul 92 restera indéterminé, et ce jusqu'en 1944.

I.5 – Quelques méthodes de construction remarquables.

Dans cette partie, nous allons étudier grossièrement différentes constructions de matrices de Hadamard. On remarquera au préalable que toute permutations de lignes et de colonnes dans une matrice de Hadamard produit toujours une matrice de Hadamard.

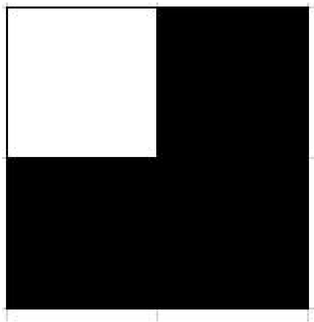
Tout d'abord, reprenons la construction de Sylvester.

Définition **:** Soit A une matrice de taille $m \times n$ et B une matrice de taille $p \times q$. On définit **le produit de Kroenecker** tel que $A \otimes B = \begin{pmatrix} a_{1\,1}.B & \cdots & a_{1\,n}.B \\ \vdots & \ddots & \vdots \\ a_{m\,1}.B & \cdots & a_{m\,n}.B \end{pmatrix}$

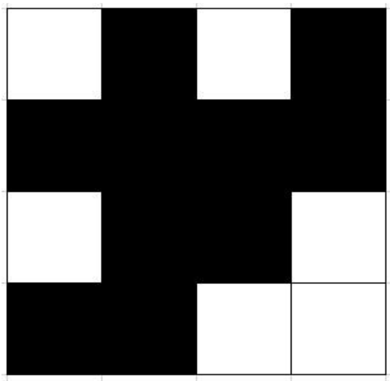
Propriété **:** Soit H_a , H_b deux matrices de $M_n(\pm 1)$, toutes deux de Hadamard.

Alors $H_{ab} = H_a \otimes H_b$ est une matrice de Hadamard.

Prenons par exemple une matrice de Hadamard de taille 2×2 :



En utilisant la méthode de Sylvester, qui consiste exactement à effectuer le produit de Kroenecker, nous obtenons la matrice de taille 4×4 suivante :

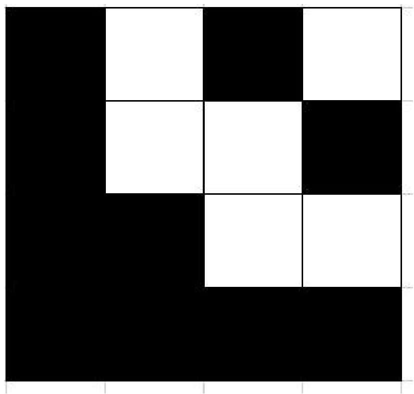


On peut faire ici plusieurs remarques. Tout d'abord, on peut vérifier que cette matrice est bien de Hadamard. Et on remarque aussi que cette matrice est différente de la matrice présentée en première sous-partie. Nous avons fait quelques lignes de codes pour créer ces matrices. (*en pièces-jointes).*

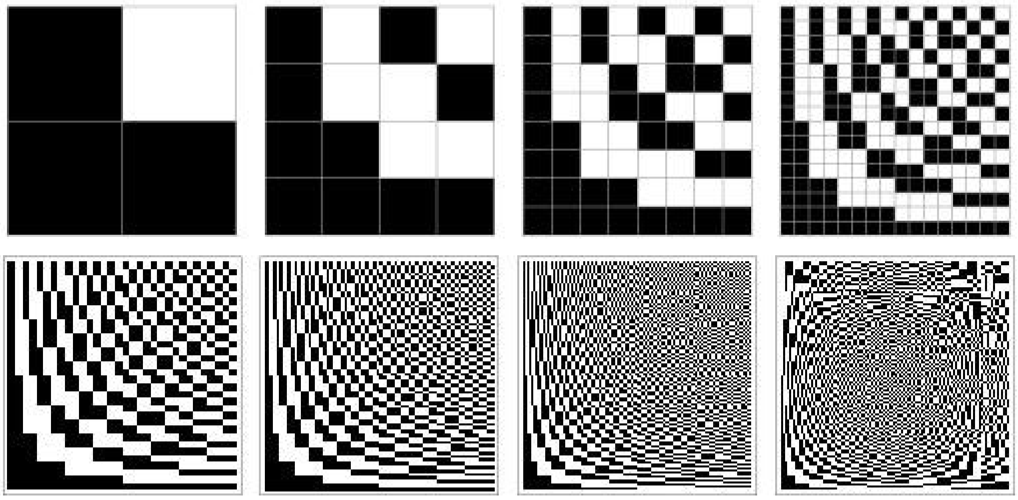
Un autre cas remarquable est la construction de matrices de Mersenne-Walsh. Ce sont des matrices de Hadamard de taille $n=2^p$, p nombre naturel. On appelle ces matrices de Mersenne puisque elles utilisent toutes les propriétés reliées aux nombres de Mersenne premiers, nombres reliées aux matrices de Hadamard par le théorème de Scarpis.

Par exemple, on peut utiliser le transformé de Walsh pour produire une matrice de Hadamard de taille 4×4 .

On obtient alors la matrice suivante :



Si l'on décide de continuer pour obtenir une structure similaire dans des ordres n grands, la série de matrices devient :



On remarque que l'on peut reproduire toutes les matrices de Walsh par permutations de lignes et de colonnes.

***

II – Étude de cas : Les matrices de presque-Hadamard.

Dans cette partie, nous nous pencherons en détail sur le concept de matrices de presque-Hadamard, découvertes par notre tuteur de projet Mr.Ion Nechita.

Cette partie est entièrement fondée sur l'article suivant ;*Some analytical aspects of Hadamard matrices* , **Ion Nechita.** Toutes les propriétés et définitions suivantes en proviennent.

Tout d'abord il advient d'introduire quelques points intéressants sur les matrices de Hadamard.

II.1 – La condition de maximisation du déterminant.

Le déterminant d'une matrice représente l'hyper-volume du parallélotope définie par les vecteurs formants les colonnes de la matrice. Ces formes géométriques à n dimensions nous aides à nous représenter une partie crucial des matrices de Hadamard.

Tout d'abord, il faut introduire la définition suivante :

Définition : Soit H une matrice de $M_n(\pm 1)$. H est **une matrice de Hadamard** si et seulement si $H \cdot H^T = n \cdot I_n$.

De cette définition, on remarque qu'une matrice de Hadamard est inversible, tel que

$$H^{-1} = \frac{1}{n} \cdot H^T \quad .$$

Nous travaillons dans l'espace des matrices carrées de taille $n \times n$ et de valeurs ± 1 . Soit donc $X \in M_n(\pm 1)$. Cette ensemble étant fini, nous avons donc tout de suite un résultat simple mais très important, $Card(M_n(\pm 1)) = 2^{n^2}$. Par exemple, le plus petit nombre multiple de 4 et inférieur à 1000 indéterminé est 668, ce qui fait 2^{446224} , qui ne peut être calculer par la très grande majorité des ordinateurs à notre disposition.

La solution qui consisterait à chercher les matrices de manière aléatoire en testant si la matrice est conforme à la définition est donc impossible. Il faut donc trouver une manière de trouver directement les matrices, en sachant où regarder.

La propriété sur le déterminant découle de la propriété suivante, l'inégalité de Hadamard.

Propriété : Soit X une matrice de taille n à coefficients complexes , et avec v_i le vecteur colonne correspondant à la $i^{ème}$ colonne de X ,alors $|det(X)|^2 \leqslant \prod_{i=1}^{n} \|v_i\|$

Dans notre cas, puisque l'on a $X \in M_n(\pm 1)$, on peut réécrire cette inégalité comme tel :

***Propriété* :** $|det(X)| \leqslant n^{\frac{n}{2}}$.

De cette inégalité découle la condition de maximisation du déterminant ;

***Propriété* :** Soit $X \in M_n(\pm 1)$, alors X est une matrice de Hadamard si et seulement si

$$|det(X)| = n^{\frac{n}{2}} \quad .$$

Démonstration c.

Cette condition implique que les matrices de Hadamard représentent des parallèlotopes particuliers, qui ont des « arêtes » orthogonales et des vecteurs compris dans les hyper-sphères unités.

Les matrices de Hadamard sont donc des matrices orthogonales et des matrices signes.

II.2 Matrices orthogonales et matrices signes.

Les matrices de Hadamard sont à l'intersection de deux ensembles bien différents. D'une part nous avons la condition si H est une matrice de Hadamard, alors $H \in M_n(\pm 1)$, H est donc une matrice signe. H appartient donc à un ensemble d'objets finis.

Mais nous avons aussi que H est la représentation d'un échiquier égalitaire, où on rappelle que les vecteurs colonnes de H sont orthogonaux entre eux. Alors, on a le $2^{ième}$ ensemble, les matrices orthogonales.

Définition **:** Soit $X \in M_n(\mathbb{R})$, X est **une matrice orthogonale** si et seulement si

$$X^T = X^{-1} .$$

On dit alors que $X \in O(n)$, l'ensemble des matrices orthogonales de taille $n \times n$.

Propriété **:** Soit $X \in M_n(\mathbb{R})$, X est une matrice de Hadamard si et seulement si

$$X \in O(n) \cap M_n(\pm 1) .$$

Ce parallèle entre ensemble fini et infini est crucial dans notre cas, puisqu'il sera l'idée de base de notre programme.

On remarque donc que le problème à une dimension géométrique très forte ; non seulement on cherche des ensembles de vecteurs tous orthogonaux entre eux, mais chacun de ces vecteurs doivent être compris dans l'hyper-sphère de dimension n . Un problème qui peut paraître simple à comprendre, mais qui devient très complexe pour $n \to +\infty$.

On comprend de plus mieux le concept de maximisation du déterminant, c'est-à-dire quels sont les familles de vecteurs compris dans l'hyper-sphère n formants un hyper-cube de dimension n ?

II.3 – Norme et propriétés.

On voit que parmi les pistes disponibles, une approche en essayant de maximiser le déterminant pourrait être prometteuse. C'est cependant tout aussi difficile que de choisir les matrices au hasard, puisque la condition implique de trouver des hyper-cubes de dimensions $n \geqslant 668$. Même si cela peut être faisable avec un temps et une puissance de calcul suffisamment grande, on ne pourrait étendre cette méthode vers l'infini.

C'est donc dans cette optique que Mr Nechita décide de trouver une seconde condition de maximisation.

Avant de commencer, il nous faut énoncer une définition et des propriétés :

Définition **:** Soit $X \in M_{n,p}(\mathbb{C})$, on définit **la norme 2** de la matrice X tel que :

$$\|X\|_2 = \sqrt{\sum_{i,j=1}^{n,p} x_{i,j}^2} \quad .$$

Propriétés **:** $\forall U \in O(n)$ et $\forall S \in M_n(\pm 1)$:

- $\|U\|_2 = \sqrt{N}$.
- $\|S\|_2 = N$.

Nous pouvons maintenant introduire la nombre h_n , tel que :

Définition **:** Soit $U \in O(n)$ et $S \in M_n(\pm 1)$, alors on peut définir h_n **le maximum de la norme 1** tel que $h_n = max \langle U | S \rangle$ ou $h_n = max \sum_{i,j=1}^{n} |u_{i,j}|$.

h_n n'est pas une fonction mais bien un nombre qui est associé aux ensembles $O(n)$ et $M_n(\pm 1)$.

Le nombre h_n représente le maximum de tout les produits scalaire entre une matrice orthogonale et une matrice unitaire. On peut donc associer à chaque n un ensemble de matrices orthogonales qui correspondent à h_n .

On peut définir maintenant une fonction tel que :

Définition **:** $\forall U \in O(n)$, on définit la fonction f , **norme 1**, tel que :

$$f : U \rightarrow \sum_{i,j=1}^{n,m} |u_{i,j}|$$

$$f : O(n) \rightarrow \mathbb{R}$$

De cette fonction, nous obtenons l'inégalité suivante :

Propriétés **:** Soit $U \in O(n)$, alors :

- $f(U) \leq n \cdot \sqrt{n}$ et immédiatement $h_n \leq n \cdot \sqrt{n}$
- Il existe une matrice de Hadamard de taille n si et seulement si $h_n = n \cdot \sqrt{n}$

Démonstration b.

Nous avons donc maintenant une propriété qui peut directement répondre à l'une des problématiques du sujet. On remarque de plus qu'il faut définir une fonction, et donc de sortir du domaine principal des matrices de Hadamard, l'algèbre linéaire.

D'après la démonstration de la condition d'égalité pour h_n , on obtient que pour chaque $U \in O(n)$ tel que $f(U) = h_n$, il existe une matrice de Hadamard A tel que $A = U \cdot \sqrt{n}$.

Dans ce cas particulier d'égalité, les matrices de Hadamard représentent les maximums globaux de f .

II.4 – Les matrices de presque-Hadamard.

Afin de trouver les maximums globaux de f , on peut chercher ses maximums locaux.

Définition **:** Soit $U \in O(n)$ tel que U est un maximum local de f , on dit que H est **une matrice de presque-Hadamard** si et seulement si $U = \frac{H}{\sqrt{n}}$.

Les matrices de presque-Hadamard existent pour toutes les dimensions n , puisque la fonction f est différentiable en tout point non nul de $O(n)$.

On peut déduire la propriété suivante :

Propriété **:** Si U est un maximum local de f , alors $\forall i, j, 1 \leq i, j \leq n$, $u_{i,j} \neq 0$.

On peut donc décider de ce placer directement dans l'ensemble des matrices orthogonales à composantes non nulles. On notera cette ensemble $O(n)^*$

II.5 – Matrice signe et partie polaire.

Les propositions suivantes sont cruciales pour le fonctionnement de l'algorithme ; il faut cependant avant poser une définition :

Définition **:** Soit $A \in M_n(\mathbb{R})$ matrice quelconque, on définit **la matrice signe** de A ,

$S \in M_n(\pm 1)$ comme $S = sign(A)$, tel que $s_{i,j} = \frac{a_{i,j}}{|a_{i,j}|}$.

Propositions **:** Soit $U \in O(n)^*$ et $S = sign(U)$ la matrice signe de U .

Alors U est :

- un point critique de f si et seulement si $U^T \cdot S$ est une matrice symétrique.
- l'antécédent d'un maximum local de f si et seulement si la somme des deux plus petites valeurs propres de U est positive.

On rappel que $A \in M_n(\mathbb{R})$ est symétrique si et seulement si $A = A^T$,et U est un point critique de f si $f'(U) = 0$.

On peut ensuite utiliser la partie polaire d'une matrice, qui est présente lors des décomposition en éléments simples, mais ceci dépasse malheureusement mon entendement.

II.6 – Algorithme

Le programme en question est disponible en pièce jointe de ce rapport.

Dans cette partie, nous allons étudier le programme qui permet de calculer, et de trouver les matrices de presque-Hadamard. Il est à noter que, quoique avancé, le programme n'est pas fini au niveau de son architecture réseau et graphe.

En reprenant le principe de transformation successive en partie polaire, puis matrice signe, on cherche à trouver et à compléter les boucles de matrices.

Le plus grand problème de cette algorithme est qu'il prend énormément de temps et de place de stockage.

Il faut donc chercher à optimiser le programme en y intégrant une structure de réseau.

***

IV – Démonstrations

a.Propriété:

$$Soit\ A \in M_n(\pm 1);\ A\ est\ une\ matrice\ de\ Hadamard \Rightarrow (n=1) \cup (n=2) \cup (n\ est\ multiple\ de\ 4)$$

Soit $A \in M_n(\pm 1)$ tel que A est une matrice de Hadamard. Si $n=1$, alors par définition il existe deux matrices de Hadamard, $A_{11}=1$ et $A_{12}=-1$, et si $n=2$, il existe au moins la matrice $A_2=\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. En supposant que A à été normalisée, c'est-à-dire que la première ligne est entièrement composée de 1, alors au moins une autre des lignes de A a autant de -1 que de 1. Il faut donc que n soit paire. Soit $n>2$; on peut toujours permuter lignes et colonnes pour réécrire A tel que :

$$A=\begin{pmatrix} 1 & & & & & \cdots & \cdots & & & & & 1 \\ 1 & & & \cdots & & 1 & -1 & & \cdots & & & -1 \\ 1 & \cdots & 1_h & -1 & \cdots & -1 & 1 & \cdots & 1_k & -1 & \cdots & -1 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & & \cdots & \cdots & & \cdots & \cdots & & \cdots & \cdots & & \cdots \end{pmatrix}.$$

Sur la deuxième ligne, nous avons exactement $\frac{n}{2}$ 1 et $\frac{n}{2}$ -1.

Supposons que sur la troisième ligne , parmis les $\frac{n}{2}$ premières composantes, il y a h 1 et $\frac{n}{2}-h$ -1, et à partir de la $\frac{n}{2}^{ième}$ composante, il y a k 1 et $\frac{n}{2}-k$ -1. Alors, puisque les lignes sont orthogonales entre elles, nous avons l'équation suivante entre la première et la troisième ligne :

$h-(\frac{n}{2}-h)+k-(\frac{n}{2}-k)=0$, dont on en déduit que $h+k=\frac{n}{2}$. De même entre la deuxième et la troisième ligne, on en déduit que $h=k=\frac{n}{2}$, il faut donc diviser n par 2 ,deux fois. n est donc divisible par 4.

b.Propriétés **:** Soit $U \in O(n)$, alors :

- $f(U)<n\sqrt{n}$ et immédiatement $h_n<n\sqrt{n}$
- Il existe une matrice de Hadamard de taille n si et seulement si $h_n=n\sqrt{n}$

En utilisant le théorème de Cauchy-Scharwtz ;Soit a et b deux éléments de $M_n(\mathbb{R})$, alors $\langle a|b\rangle \leqslant \|a\|.\|b\|$, on peut écrire :

$$f(U)=\sum_{i,j=1}^{n} |u_{i,j}| \leq \sqrt{\sum_{i,j=1}^{n} u_{i,j}^2}.\sqrt{\sum_{i,j=1}^{n} 1^2}=n\sqrt{n}$$

Le cas d'égalité correspond au cas où $|u_{i,j}|=constante$, c'est-à-dire au moment où chacune des composantes de U sont maximales, ici c'est le cas où $|u_{i,j}|=\frac{1}{\sqrt{n}}$, et donc c'est-à-dire si $A=U\sqrt{n}$ est une matrice de Hadamard.

c.Propriété **:** Soit $X \in M_n(\pm 1)$, alors X est une matrice de Hadamard si et seulement si

$$|det(X)| = n^{\frac{n}{2}}$$

Soit H une matrice de Hadamard de taille n , et $d = det\, H$. Si l'on divise toutes les lignes par $\sqrt{n}$, on obtient une matrice orthogonale B de déterminant $b = \frac{d}{\sqrt{n}^n} = \pm 1$. Directement, on a $|d| = n^{\frac{n}{2}}$.

***

Références

Application of 4k-order Hadamard Matrices to Simultaneous Driving Capacitive Touch Systems, **Jong Kang Park 2015**

[01] *Generalization of Scarpis's theorem on Hadamard matrices,* **Dragomir Z, Dokovic 2016**

La conjecture de Hadamard (I) **Shalom Eliahou, CNRS Image des Mathématiques ;https://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html**

On the Existence of Hadamard Matrices **Jennifer Seberry Wallis 1975**

Some analytical aspects of Hadamard matrices **Ion Nechita 2016**

Almost Hadamard matrices: general theory and examples **T. Banica, I. Nechita, K. Zyczkowski - Open Systems & Information Dynamics, Vol. 19, No. 4, 1250024 (2012)**

http://mathworld.wolfram.com/HadamardMatrix.html

https://math.stackexchange.com/questions/2715871/determinant-of-a-hadamard-matrix-as-a-function-of-n