La conjecture de Hadamard

Shalom Eliahou

Université du Littoral Côte d'Opale

LIPN, Séminaire CALIN, 5 février 2013

Introduction

Définition

Une *matrice de Hadamard* est une matrice carrée à coefficients ± 1, orthogonale à un facteur scalaire près.

Autrement dit, $\langle L_i \mid L_j \rangle = 0$ pour tout $i < j$.

Exemples

$$(+), \quad \begin{pmatrix} + & + \\ + & - \end{pmatrix}, \quad \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}.$$

Motivation (Hadamard, 1893)

Maximisation du déterminant

Soit B matrice carrée d'ordre n à coefficients dans l'intervalle $[-1, 1]$. Alors

$$|\det(B)| \leq n^{n/2},$$

avec égalité $\Longleftrightarrow$ B est une matrice de Hadamard.

Question.

Quels sont les ordres possibles $n \in \mathbb{N}$ des matrices de Hadamard ?

Condition nécessaire.

$n \leq 2$ ou $n \equiv 0 \bmod 4$.

Conjecture (Hadamard, 1893)

Pour tout $n \equiv 0 \bmod 4$, il existe une matrice de Hadamard d'ordre n.

Derniers cas ouverts sous 1000 : 668, 716, 892.

Transformations faciles

Les transformations suivantes préservent les matrices de Hadamard :

- Permuter les lignes, permuter les colonnes.
- Multiplier une ligne par -1, multiplier une colonne par -1.

Application

On peut toujours *normaliser* une matrice de Hadamard, i.e. rendre sa première ligne et sa première colonne constantes à 1 :

$$H = \left(\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \end{array}\right).$$

Sylvester (1867)

Théorème

Pour tout $n = 2^r$, il existe une matrice de Hadamard d'ordre n.

Preuve. Si A est une matrice de Hadamard d'ordre n, alors

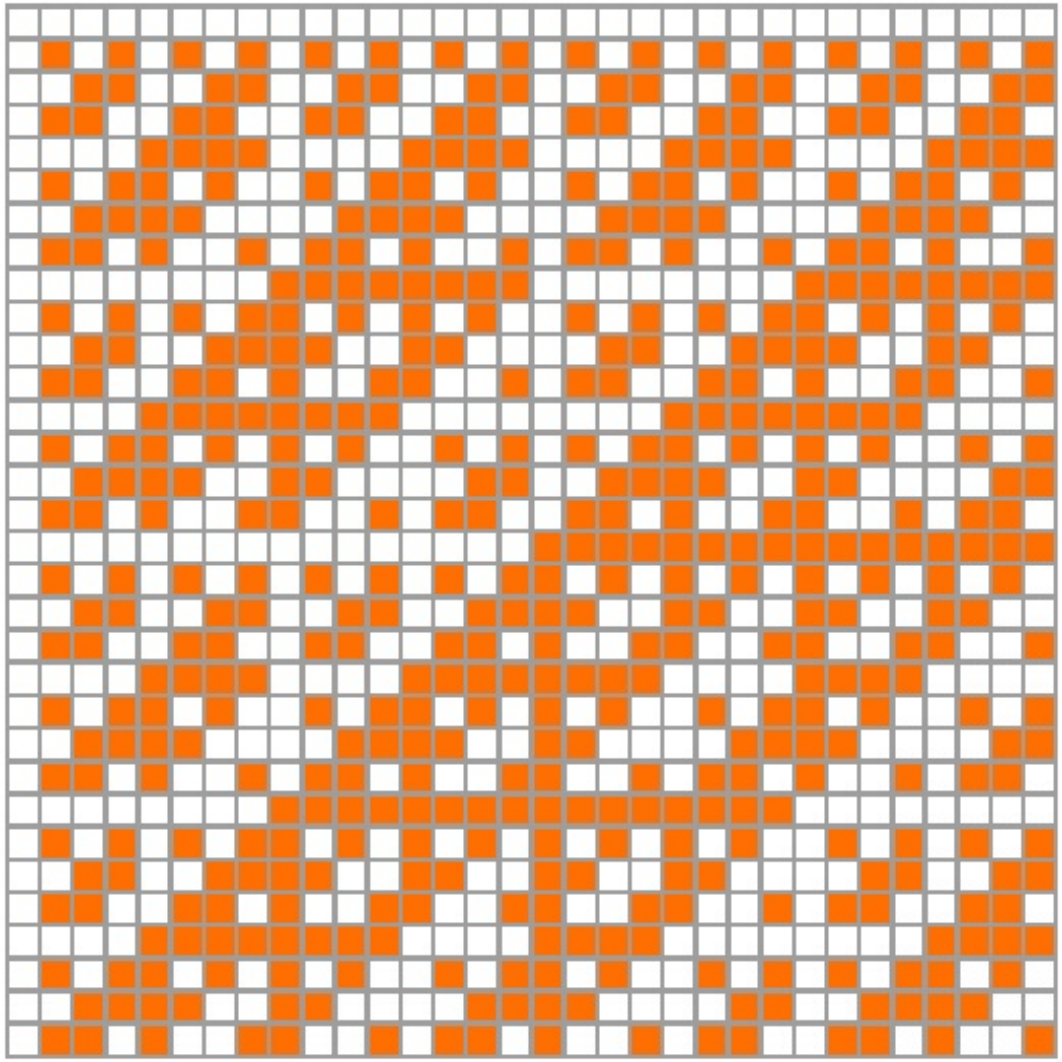
$$\begin{pmatrix} A & A \\ A & -A \end{pmatrix}.$$

est une matrice de Hadamard d'ordre $2n$. □

Théorème

Le produit tensoriel de matrices de Hadamard d'ordres n_1 et n_2 est une matrice de Hadamard d'ordre $n_1 n_2$.

Sylvester d'ordre 32



Hadamard (1893)

Construction combinatoire de matrices de Hadamard d'ordre 12 et 20.

Voici celle pour $n = 12$. Les 3 premières lignes sont :

$$
\begin{array}{cccccccccccc}
+ & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & - & - & - & - & - & - \\
+ & + & + & - & - & - & + & + & + & - & - & -
\end{array}
$$

Les 9 lignes restantes sont décrites par le tableau

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

dans lequel on remplace

- les 1 par $-++$ dans C1 & C4, et par $+--$ dans C2 & C3
- les 2 par $+-+$ dans C1 & C4, et par $-+-$ dans C2 & C3
- les 3 par $++-$ dans C1 & C4, et par $--+$ dans C2 & C3

Scarpis (1898)

Théorème

Soit $n \equiv 0 \bmod 4$ tel que $n-1$ premier. S'il existe une matrice de Hadamard d'ordre n, alors il en existe une d'ordre $(n-1)n$.

Donc, il existe des matrices de Hadamard d'ordre $12 = 3 \cdot 4$ et d'ordre $56 = 7 \cdot 8$.

Corollaire

Si $2^k - 1$ est un premier de Mersenne, alors il existe une matrice de Hadamard d'ordre $(2^k - 1)2^k$.

[On connaît 47 premiers de Mersenne à ce jour. Le plus grand parmi eux est $2^{43\,112\,609} - 1$.]

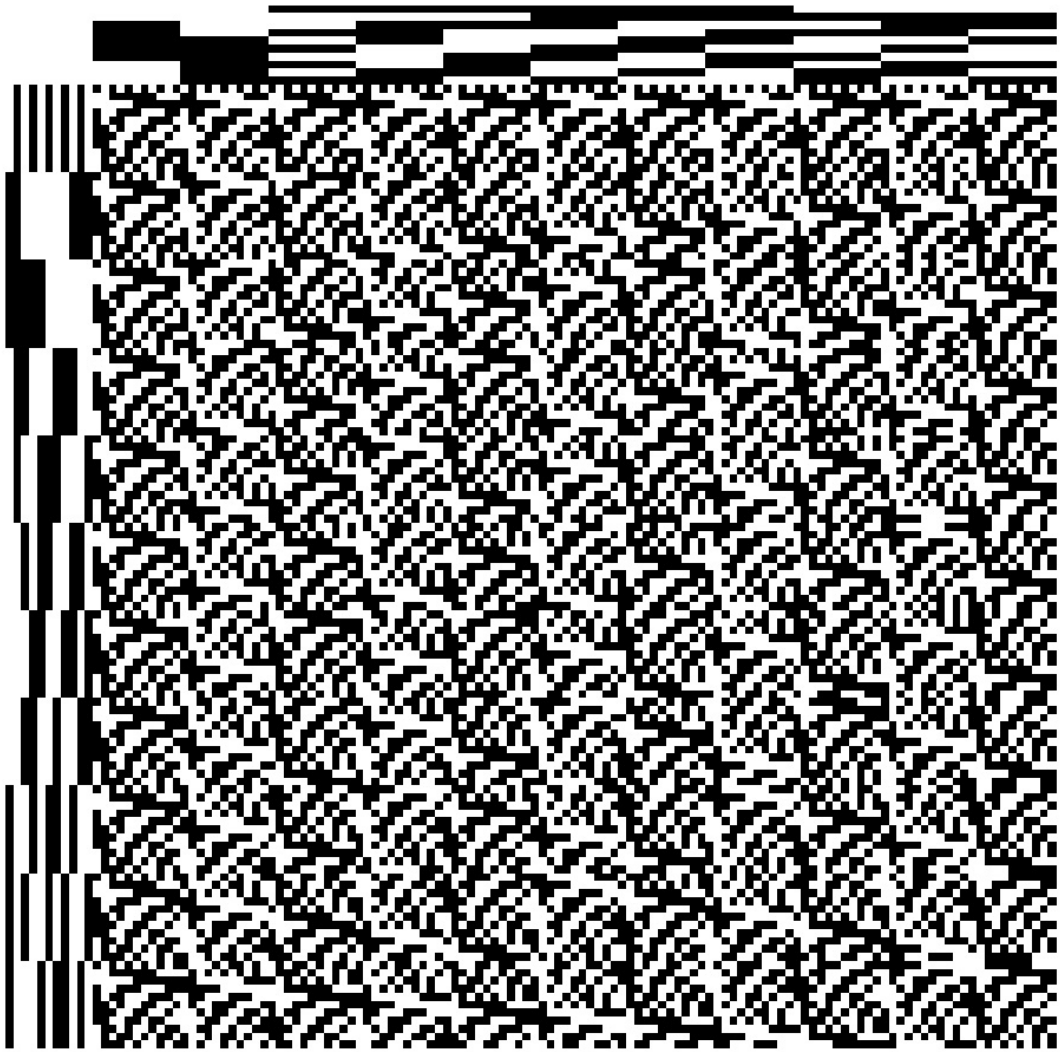
Parfois, on peut itérer Scarpis, tant que $n-1$ reste premier :

$$\begin{aligned} 4 &\longmapsto 3 \cdot 4 = 12 \\ &\longmapsto 11 \cdot 12 = 132 \\ &\longmapsto 131 \cdot 132 = 17\,292 \\ &\longmapsto 17291 \cdot 17\,292 = 298\,995\,972. \end{aligned}$$

Scarpis fournit donc une matrice de Hadamard d'ordre

$$298\,995\,972 = 2^2 \cdot 3 \cdot 11 \cdot 131 \cdot 17\,291.$$

Scarpis d'ordre 132



La construction de Scarpis

Soit H une matrice de Hadamard H d'ordre n. On va en fabriquer une plus grande, d'ordre $(n-1)n$.

► Tout d'abord, on "explose" H en $\widehat{H}$: on remplace chaque coefficient ε de H par la ligne constante $(\varepsilon,\ldots,\varepsilon)$ de longueur $n-1$:

$$\varepsilon \longmapsto (\underbrace{\varepsilon,\ldots,\varepsilon}_{n-1}).$$

Ainsi, $\widehat{H}$ a n lignes comme H, et $(n-1)n$ colonnes :

$$\widehat{H} = H \otimes (1,1,\ldots,1).$$

Ses lignes sont 2 à 2 orthogonales.

▶ Revenons à H : on peut supposer que H est normale :

$$H = \left(\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & H' & \\ 1 & & & \end{array}\right).$$

On appelle H' le coeur de H. C'est une matrice carrée d'ordre $n-1$. On peut aussi supposer que $L_2(H)$ *est alternée* :

$$L_2(H) = (1,-1,1,-1,\ldots,1,-1).$$

▶ Nommons ainsi les lignes de H' :

$$H' = \begin{pmatrix} -A_1 \\ -A_2 \\ \vdots \\ -A_{n-1} \end{pmatrix}.$$

▶ On va construire notre matrice M d'ordre $(n-1)n$ ainsi :

$$M = \left(\begin{array}{c} M_0 \\ \hline M_1 \\ \hline \vdots \\ \hline M_{n-1} \end{array}\right),$$

chaque M_i ayant $n-1$ lignes et $(n-1)n$ colonnes.

▶ On pose M_0 = la matrice explosée $\widehat{H}$ dont on supprime la 2ème ligne, à savoir

$$(\underbrace{1,\ldots,1}_{n-1},\underbrace{-1,\ldots,-1}_{n-1},\ldots,\underbrace{-1,\ldots,-1}_{n-1}).$$

Ainsi, M_0 a bien la taille requise, soit $n-1$ lignes et $(n-1)n$ colonnes.

- On pose

$$M_1 = \begin{pmatrix} A_1 & -A_1 & A_1 & -A_1 & \cdots & -A_1 \\ A_1 & -A_2 & A_2 & -A_2 & \cdots & -A_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_1 & -A_{n-1} & A_{n-1} & -A_{n-1} & \cdots & -A_{n-1} \end{pmatrix}.$$

- Plus généralement, pour tout $1 \leq r \leq n-1$, on pose

$$M_r = \begin{pmatrix} A_r & -A_1 & A_{1+(r-1)} & \cdots & \cdots \\ A_r & -A_2 & A_{2+(r-1)} & \cdots & \cdots \\ \vdots & \vdots & \vdots & (-1)^j A_{i+(j-1)(r-1)} & \vdots \\ A_r & -A_{n-1} & A_{n-1+(r-1)} & \cdots & \cdots \end{pmatrix}$$

pour tout $1 \leq i, j \leq n-1$.

- *Alors, la matrice ainsi construite,*

$$M = \left(\begin{array}{c} M_0 \\ \hline M_1 \\ \hline \vdots \\ \hline M_{n-1} \end{array}\right),$$

est une matrice de Hadamard d'ordre $(n-1)n$.

Gilman

L'hypothèse d'existence du théorème de Scarpis est toujours satisfaite !

Théorème (Gilman, 1930)

Soit $n \equiv 0 \bmod 4$ tel que $n-1$ soit premier. Alors il existe une matrice de Hadamard d'ordre n.

Clé : la répartition des carrés parfaits dans le corps $\mathbb{Z}/(n-1)\mathbb{Z}$.

Hélas, pas d'article publié. Juste un résumé dans les compte-rendus d'une grande conférence de l'AMS fin décembre 1930 à Cleveland, Ohio.

Paley

Théorème (Paley, 1933)

Soit $n \equiv 0 \bmod 4$ tel que $n-1$ soit une puissance de premier. Alors il existe une matrice de Hadamard d'ordre n.

Clé : la répartition des carrés parfaits dans le corps fini $\mathbb{F}_{n-1}$. En effet, posons $q = n-1 = p^r$, et

$$\begin{array}{rccll} \chi & : & \mathbb{F}_q & \longrightarrow & \{0, \pm 1\} \\ & & 0 & \longmapsto & 0 \\ & & x & \longmapsto & 1 \qquad \text{si } x \neq 0 \text{ est un carré parfait,} \\ & & x & \longmapsto & -1 \qquad \text{sinon.} \end{array}$$

Matrice de Hadamard d'ordre n, pour $n \equiv 0 \bmod 4$ et $n-1 = p^r = q$:

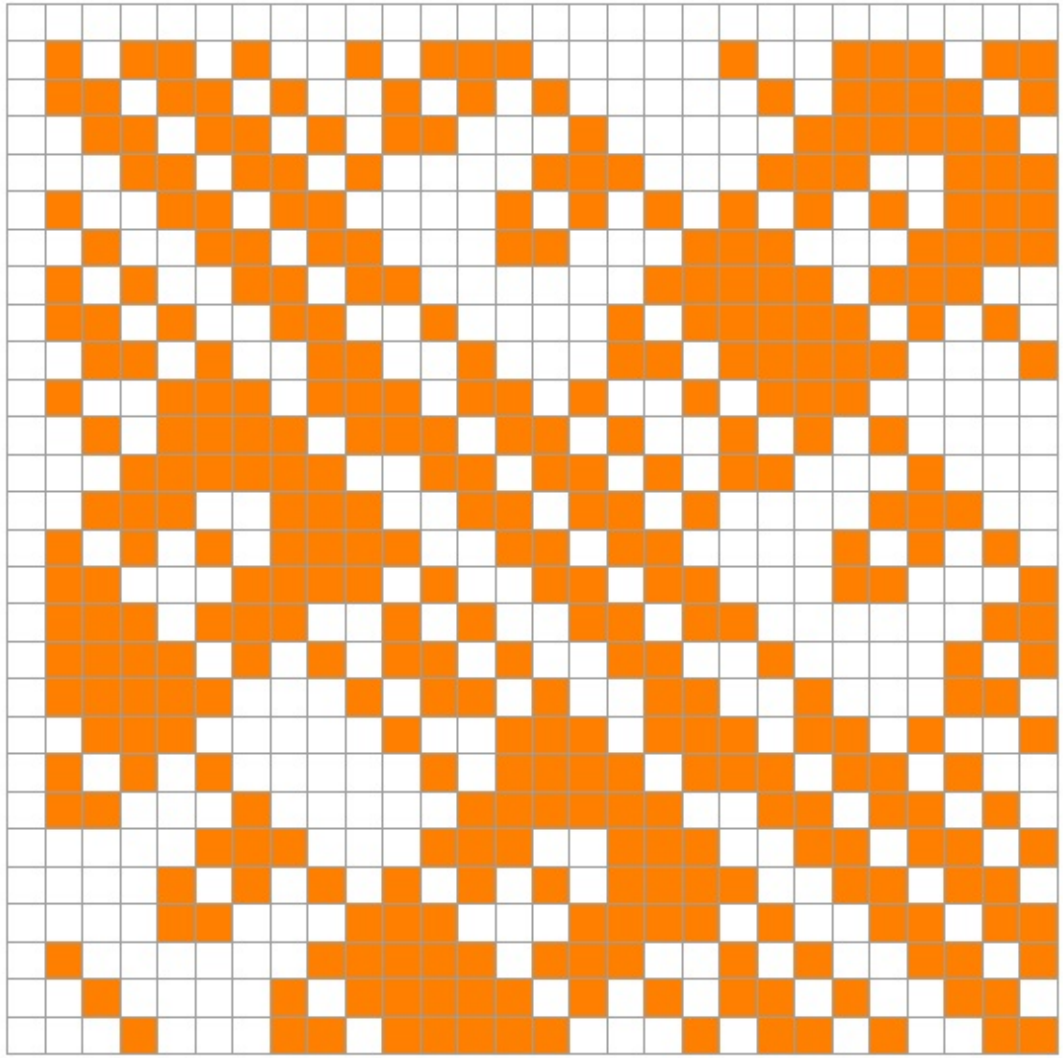
$$H = \left(\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & \left(\chi'(i-j)\right)_{i,j\in\mathbb{F}_q} & \\ 1 & & & \end{array}\right),$$

où $\chi' = \chi$ sur $\mathbb{F}_q^*$ et $\chi'(0) = -1$.

Lemme clé

- $\chi(xy) = \chi(x)\chi(y)$ pour tout $x, y \in \mathbb{F}_q$,
- $\sum_{x\in\mathbb{F}_q} \chi(x) = 0$,
- $\sum_{x\in\mathbb{F}_q} \chi(x)\chi(x+a) = -1$ pour tout $a \in \mathbb{F}_q^*$.

Hadamard d'ordre 28 basée sur $\mathbb{F}_{27}$



Seberry

Théorème (Seberry, 1976)

Pour tout $m \in \mathbb{N}$ impair, il existe une matrice de Hadamard d'ordre $2^t m$ pour tout entier t assez grand.

Idée : assemblage astucieux de blocs carrés de la forme

$$J_q = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & & 1 \end{pmatrix}, \quad J'_q = \begin{pmatrix} -1 & 1 & \cdots & 1 \\ 1 & -1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & & -1 \end{pmatrix}$$

et $\Big(\chi(i-j)\Big)_{i,j\in\mathbb{F}_q}$.

Un autre ingrédient de la preuve de Seberry est le théorème de Sylvester sur les semigroupes numériques $S = \langle a, b \rangle = \mathbb{N}a + \mathbb{N}b$.

Théorème (Sylvester, $\sim$1865)

Soient $a, b \in \mathbb{N}$ premiers entre eux. Alors tout entier $N \geq (a-1)(b-1)$ appartient à $S = \mathbb{N}a + \mathbb{N}b$.

Exemple

$\langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \rightarrow\}$

Spécifications économiques

Objectif

Pour $n \in 4\mathbb{N}$, construire une matrice de Hadamard d'ordre n en spécifiant beaucoup moins que n^2 coefficients.

Par exemple, une matrice **circulante** d'ordre n est n spécifiée par seulement n coefficients, ceux de sa 1ère ligne.

Existe-t-il des matrices de Hadamard circulantes ? Oui :

$$\mathrm{circ}(-1,1,1,1) = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Ryser, Turyn

Conjecture (Ryser, 1960)

Il n'existe aucune matrice de Hadamard circulante d'ordre $n > 4$.

Théorème (Turyn, 1965)

S'il existe une matrice de Hadamard circulante d'ordre $n \geq 4$, alors $n = 4m^2$ avec m impair (plus d'autres restrictions sur m).

Approche : théorie algébrique des nombres, étude des entiers cyclotomiques $\mathbb{Z}[e^{2i\pi/n}]$.

Turyn, Schmidt, Leung, Mossinghoff, etc. : conjecture vraie pour $n \leq 10^9$, sauf éventuellement pour $n = 4 \times 117\,152 = 548\,964\,900$.

Turyn

Un quadruple de suites binaires de longueur m permet, sous certaines conditions, de fabriquer une matrice de Hadamard d'ordre $n = 4m$.

Définition

Soit $A = (a_0, a_1, \ldots, a_{m-1})$ une suite réelle de longueur m. Pour $0 \leq s \leq m-1$, le s-ème coefficient de corrélation apériodique de A est

$$c_s(A) = \sum_{i=0}^{m-1-s} a_i a_{i+s}.$$

Cette somme compte $m - s$ termes. Par exemple,

$$\begin{aligned} c_1(A) &= a_0 a_1 + a_1 a_2 + \cdots + a_{m-2} a_{m-1}, \\ c_{m-1}(A) &= a_0 a_{m-1}. \end{aligned}$$

Définition

Un quadruple de Turyn est un quadruple de suites binaires (A, B, C, D) de longueur m telles que, pour tout $1 \leq s \leq m-1$, on a

$$c_s(A) + c_s(B) + c_s(C) + c_s(D) = 0.$$

Exemple : (S_1, S_2, S_3, S_3) est un quadruple de Turyn, où

$$\begin{aligned} S_1 &= +++ \\ S_2 &= +-+ \\ S_3 &= ++-. \end{aligned}$$

En effet, voici les corrélations de ces suites :

X	c_1	c_2
$+++$	2	1
$+-+$	-2	1
$++-$	0	-1

Théorème (Goethals-Seidel, 1970)

Si (A, B, C, D) est un quadruple de Turyn de longueur m, alors la matrice suivante d'ordre $n = 4m$ est de Hadamard :

$$\begin{pmatrix} A & -BR & -CR & -DR \\ BR & A & -D^\top R & C^\top R \\ CR & D^\top R & A & -B^\top R \\ DR & -C^\top R & B^\top R & A \end{pmatrix},$$

où A, B, C, D dénotent les circulantes respectives des suites, et où

$$R = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \diagup & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Conjecture (Turyn, $\sim$1974)

Pour tout $m \in \mathbb{N}$, il existe un quadruple de Turyn de longueur m.

Fait remarquable :

$$\text{Conjecture de Turyn} \implies \begin{cases} \text{Conjecture de Hadamard,} \\ \text{Théorème des 4 carrés de Lagrange.} \end{cases}$$

Preuve de Turyn $\implies$ Lagrange :

A la suite $A = (a_0, a_1, \ldots, a_{m-1})$, on associe le polynôme

$$A(z) = a_0 + a_1 z + \cdots + a_{m-1} z^{m-1}.$$

Alors

$$A(z)A(z^{-1}) = \sum_{s=0}^{m-1} c_s(A)(z^s + z^{-s}).$$

Conséquence

Soit (A, B, C, D) un quadruple de suites binaires de longueur m. Alors (A, B, C, D) *est de Turyn si et seulement si*

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) + C(z)C(z^{-1}) + D(z)D(z^{-1}) = 4m.$$

En posant $z = 1$, cela donne

$$4m = A(1)^2 + B(1)^2 + C(1)^2 + D(1)^2.$$

Donc $4m$ est une somme de 4 carrés. Donc m aussi. □

Un affaiblissement modulaire

Ici, on n'exige plus $\langle L_i \mid L_j \rangle = 0$, mais seulement $\langle L_i \mid L_j \rangle \equiv 0 \bmod m$.

Définition (Marrero-Butson, $\sim$1970)

Soit $m \in \mathbb{N}$. Une matrice de Hadamard m-modulaire est une matrice à coefficients ± 1 et à lignes 2 à 2 orthogonales modulo m.

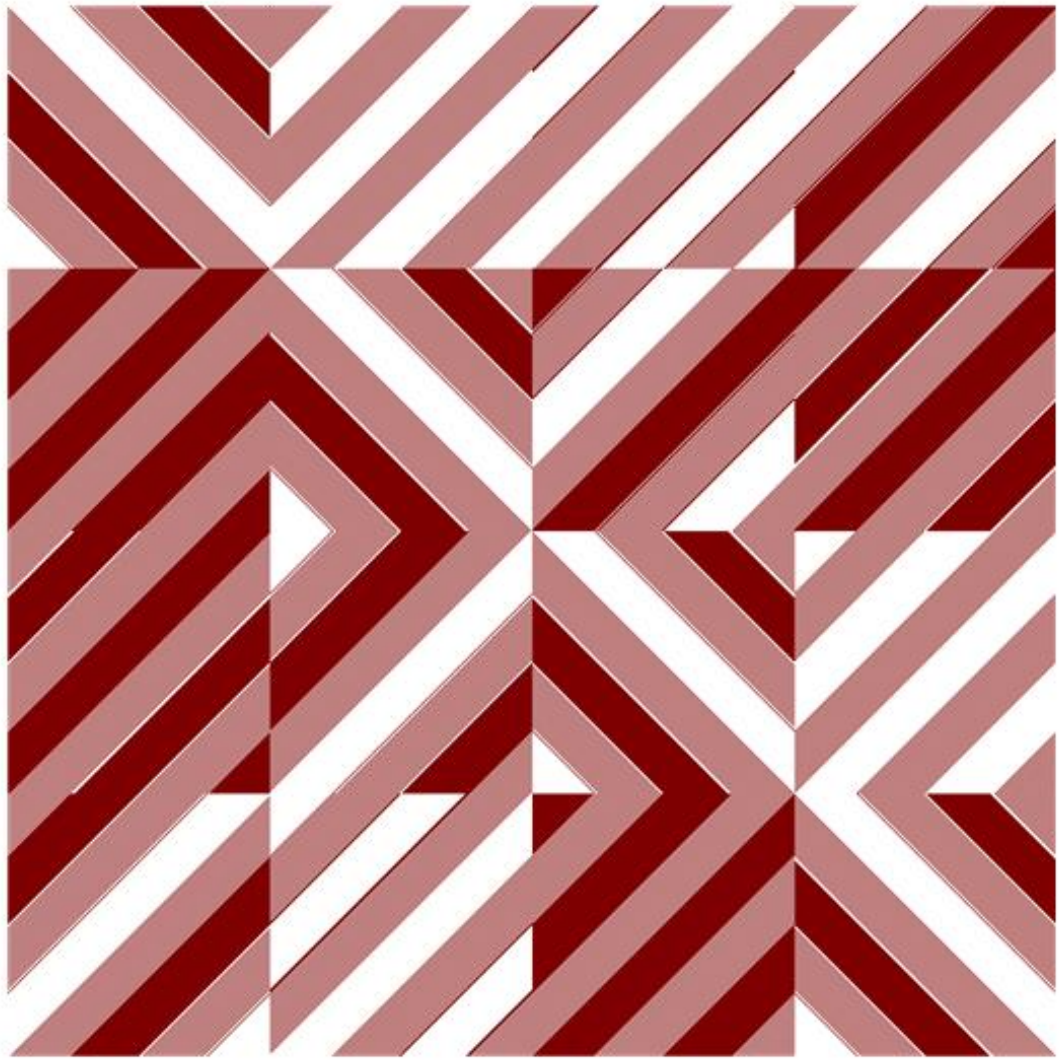
La conjecture de Hadamard m-modulaire

Pour tout $n \in 4\mathbb{N}$, il existe une matrice de Hadamard m-modulaire d'ordre n.

Marrero-Butson (1972) : vrai pour $m = 12$.

E-Kervaire (2001) : vrai pour $m = 32$.

Une Hadamard 32-modulaire d'ordre 668



Proposition

La conjecture de Hadamard est vraie si et seulement si sa version m-modulaire est vraie pour une infinité de modules m.

Preuve

- Si $k =$ le produit scalaire de deux lignes d'une matrice binaire A d'ordre n, alors $|k| \leq n$.
- De plus, si A est m-modulaire, alors $k \equiv 0 \bmod m$.
- Donc si $m > n$, alors $k = 0$, puisque $m > n \geq |k|$. $\square$

Wanted : La version 64-modulaire de la conjecture de Hadamard !

Images : site Images des Mathématiques, images.math.cnrs.fr.

Merci pour votre attention.