The Hadamard conjecture

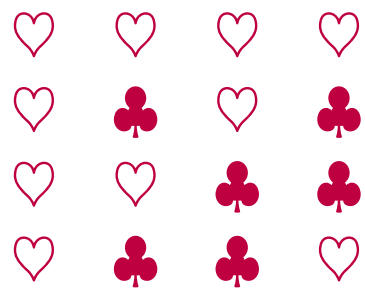
Teo Banica

"Introduction to Hadamard matrices", 1/6

07/20

Hadamard matrices

Sylvester. Arrays having the property that when comparing 2 rows, the number of matchings equals the number of mismatchings:



Definition. An Hadamard matrix is a square binary matrix $H \in M_N(\pm 1)$ whose rows are pairwise orthogonal.

Remark. We must have $H \in M_N(\pm 1) \cap \sqrt{N} O_N$, and so the columns must be pairwise orthogonal too.

Walsh matrices

The simplest example of an Hadamard matrix is:

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Tensor product operation, using double indices:

$$(H \otimes K)_{ia,jb} = H_{ij} K_{ab}$$

We can tensor W_2 with itself. With lexicographic order:

$$W_2 \otimes W_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\Longrightarrow$ Walsh matrices $W_N = W_2^{\otimes n}$, of size $N = 2^n$. Radio, coding.

General theory

Theorem. The Hadamard matrices are stable under:

(1) Permuting rows, or permuting columns.

(2) Switching signs on rows, or on columns.

(3) Taking the transpose.

(4) Making tensor products.

Proof. All this is clear from $H \in M_N(\pm 1) \cap \sqrt{N} O_N$, because all operations preserve both $M_N(\pm 1)$ and $\sqrt{N} O_N$.

Convention. Two Hadamard matrices are called equivalent, $H \sim K$, when we can pass from one to the other via (1,2).

Hadamard bound

Theorem. Given a matrix $H \in M_N(\pm 1)$, we have

$$|\det(H)| \leq N^{N/2}$$

with equality precisely when H is Hadamard.

Proof. The determinant of a system of N vectors in $\mathbb{R}^N$ is:

$$\det(H_1, \ldots, H_N) = \pm vol < H_1, \ldots, H_N >$$

In our case, ± 1 entries, we have the following inequality,

$$|\det(H_1, \ldots, H_N)| \leq ||H_1|| \times \ldots \times ||H_N|| = (\sqrt{N})^N$$

with equality when our vectors are pairwise orthogonal.

Norm estimates

Theorem. Given a matrix $U \in O_N$, we have

$$||U||_1 \leq N\sqrt{N}$$

with equality precisely when $H = U/\sqrt{N}$ is Hadamard.

Proof. We have the following Cauchy-Schwarz estimate:

$$||U||_1 = \sum_{ij} |U_{ij}| \leq N \left(\sum_{ij} |U_{ij}|^2 \right)^{1/2} = N\sqrt{N}$$

The equality case holds when $|U_{ij}| = \sqrt{N}$ for any i, j, and so when the rescaled matrix $H = U/\sqrt{N}$ satisfies $H \in M_N(\pm 1)$.

Size restriction

Theorem. The size of an Hadamard matrix is $N \in \{2\} \cup 4\mathbb{N}$.

Proof. Permute rows/columns, multiply them by -1:

$$H = \begin{pmatrix} 1 \ldots\ldots 1 & 1 \ldots\ldots 1 & 1 \ldots\ldots 1 & 1 \ldots\ldots 1 \\ 1 \ldots\ldots 1 & 1 \ldots\ldots 1 & -1 \ldots -1 & -1 \ldots -1 \\ 1 \ldots\ldots 1 & -1 \ldots -1 & 1 \ldots\ldots 1 & -1 \ldots -1 \\ \underbrace{\cdots\cdots\cdots}_{x} & \underbrace{\cdots\cdots\cdots}_{y} & \underbrace{\cdots\cdots\cdots}_{z} & \underbrace{\cdots\cdots\cdots}_{t} \end{pmatrix}$$

The orthogonality conditions between the first 3 rows read:

$$x+y=z+t \quad , \quad x+z=y+t \quad , \quad x+t=y+z$$

Solution $x=y=z=t \implies 4|N$.

Case $N \notin 4\mathbb{N}$

What to do? There are two possible choices here:

Definition 1. A quasi-Hadamard matrix is a matrix

$$H \in M_N(\pm 1)$$

which maximizes the quantity $|\det(H)|$.

Definition 2. An almost Hadamard matrix is a matrix

$$H \in \sqrt{N} O_N$$

which maximizes the quantity $||H||_1$.

Hadamard conjecture

Conjecture (HC). There is at least one Hadamard matrix

$$H \in M_N(\pm 1)$$

for any integer $N \in 4\mathbb{N}$.

(1) OK for $N = 4, 8, 16, 32, 64, \ldots$ (Walsh)

(2) Many other constructions (human, computer)

(3) $\#\{Hadamard\}$ grows exponentially with N. We just need one!

Verification as of 2020 goes up to the number of the beast:

$$\mathfrak{N} = 666$$

(That is, $N \leq 664$ known, $N = 668$ unknown. No joke here!)

Paley matrices

Define $\chi : \mathbb{F}_q \to \{-1, 0, 1\}$ by $\chi(0) = 0$, $\chi(a) = 1$ if $a = b^2$ for some $b \neq 0$, and $\chi(a) = -1$ otherwise. Set $Q_{ab} = \chi(a - b)$.

(1) Paley 1: if $q = 3(4)$ we have a matrix of size $N = q + 1$:

$$P_N^1 = 1 + \begin{pmatrix} 0 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & Q & \\ -1 & & & \end{pmatrix}$$

(2) Paley 2: if $q = 1(4)$ we have a matrix of size $N = 2q + 2$:

$$P_N^2 = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{pmatrix} \ : \ 0 \to \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \ , \ \pm 1 \to \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Skew-symmetric ($H + H^t = 2$), respectively symmetric ($H = H^t$).

Proof 1/3

We denote by 1 all identity matrices, of any size, and by $\mathbb{I}$ all rectangular all-one matrices, of any size as well. We have:

$$QQ^t = q1 - \mathbb{I} \quad , \quad Q\mathbb{I} = \mathbb{I}Q = 0$$

In addition, we have the following formulae, coming from the fact that -1 is a square in $\mathbb{F}_q$ precisely when $q = 1(4)$:

$$q = 1(4) \implies Q = Q^t$$

$$q = 3(4) \implies Q = -Q^t$$

With these observations in hand, the proof goes as follows:

Proof 2/3

(1) With our conventions, the matrix in the statement is:

$$P_N^1 = \begin{pmatrix} 1 & \mathbb{I} \\ -\mathbb{I} & 1+Q \end{pmatrix}$$

The Hadamard matrix condition follows from:

$$\begin{aligned} P_N^1 (P_N^1)^t &= \begin{pmatrix} 1 & \mathbb{I} \\ -\mathbb{I} & 1+Q \end{pmatrix} \begin{pmatrix} 1 & -\mathbb{I} \\ \mathbb{I} & 1-Q \end{pmatrix} \\ &= \begin{pmatrix} N & 0 \\ 0 & \mathbb{I}+1-Q^2 \end{pmatrix} \\ &= \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix} \end{aligned}$$

The fact that our matrix is skew-symmetric is clear as well.

Proof 3/3

If we denote by G, F the matrices in the statement, which replace respectively the $0, 1$ entries, our matrix is given by:

$$P_N^2 = \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes F + 1 \otimes G$$

The Hadamard matrix condition follows from:

$$\begin{aligned} & (P_N^2)^2 \\ = & \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix}^2 \otimes F^2 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes G^2 + \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes (FG + GF) \\ = & \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \otimes 2 + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes 2 + \begin{pmatrix} 0 & \mathbb{I} \\ \mathbb{I} & Q \end{pmatrix} \otimes 0 \\ = & \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix} \end{aligned}$$

The fact that our matrix is symmetric is clear as well.

Applications

Theorem. The HC is verified at least up to $N = 88$, as follows:

(1) At $N = 4, 8, 16, 32, 64$ we have Walsh matrices.

(2) At $N = 12, 20, 24, 28, 44, 48, 60, 68, 72, 80, 84, 88$ we have Paley 1 matrices.

(3) At $N = 36, 52, 76$ we have Paley 2 matrices.

(4) At $N = 40, 56$ we have Paley 1 matrices tensored with W_2.

At $N = 92$ these constructions (Walsh, Paley, $\otimes$) don't work.

Williamson matrices

Theorem. Assuming that $A, B, C, D \in M_K(\pm 1)$ are circulant, symmetric, pairwise commute and satisfy

$$A^2 + B^2 + C^2 + D^2 = 4K$$

the following $4K \times 4K$ matrix is Hadamard:

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

Moreover, such a matrix exists at $K = 23$, and so at $N = 92$.

Proof

With $1, i, j, k \in M_4(0,1)$ being the quaternion units, we have:

$$H = A \otimes 1 + B \otimes i + C \otimes j + D \otimes k$$

Assuming now that A, B, C, D are symmetric, we have:

$$\begin{aligned} HH^t &= (A \otimes 1 + B \otimes i + C \otimes j + D \otimes k) \\ &\quad (A \otimes 1 - B \otimes i - C \otimes j - D \otimes k) \\ &= (A^2 + B^2 + C^2 + D^2) \otimes 1 - ([A,B] - [C,D]) \otimes i \\ &\quad -([A,C] - [B,D]) \otimes j - ([A,D] - [B,C]) \otimes k \end{aligned}$$

Thus, if we further assume that A, B, C, D commute, and satisfy $A^2 + B^2 + C^2 + D^2 = 4K$, we obtain an Hadamard matrix.

Circulant A, B, C, D were found at $K = 23$ by a computer search.

Cocyclic matrices

Definition. A cocycle on G is a matrix $H \in M_G(\pm 1)$ satisfying:

$$H_{11} = 1 \quad , \quad H_{gh} H_{gh,k} = H_{g,hk} H_{hk}$$

When rows are orthogonal, we say that H is cocyclic Hadamard.

Example. The Walsh matrix $H = W_{2^n}$ is cocyclic, coming from the group $G = \mathbb{Z}_2^n$, with cocycle $H_{gh} = (-1)^{<g,h>}$.

Conjecture (Cocyclic HC). There is at least one cocyclic Hadamard matrix $H \in M_N(\pm 1)$, for any $N \in 4\mathbb{N}$.

Circulant matrices

Conjecture (CHC). The only circulant Hadamard matrices are

$$K_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

and its conjugates. In other words, no circulants at $N > 4$.

If we denote by $S \subset \{1, \ldots, N\}$ the set of positions of the -1 entries in the first row, we are led to:

Conjecture (Ryser). At $N > 4$, there is no set $S \subset \{1, \ldots, N\}$,

$$|S \cap (S + k)| = |S| - N/4$$

for any $k \neq 0$, taken modulo N.

De Launey-Levin

Definition. A partial Hadamard matrix (PHM) is a matrix

$$H \in M_{M\times N}(\pm 1)$$

having its rows pairwise orthogonal.

Theorem. The probability for $H \in M_{M\times N}(\pm 1)$ to be PHM is

$$P_M \simeq \frac{2^{(M-1)^2}}{\sqrt{(2\pi N)^{\binom{M}{2}}}}$$

in the $N \in 4\mathbb{N}$, $N \to \infty$ limit.

Proof (idea)

The probability for $H \in M_{M\times N}(\pm 1)$ to be PHM is the probability for a length N random walk with increments drawn from

$$E = \left\{ (e_i \bar{e}_j)_{i<j} \middle| e \in \mathbb{Z}_2^M \right\}$$

regarded as subset $\mathbb{Z}_2^{\binom{M}{2}}$, to return at the origin. This gives:

$$P_M = \frac{1}{q^{(M-1)N}} \sum_{\xi_1,\ldots,\xi_N \in E} \delta_{\Sigma\xi_i,0}$$

By Fourier inversion we have, with $D = \binom{M}{2}$:

$$\delta_{\Sigma\xi_i,0} = \frac{1}{(2\pi)^D} \int_{[-\pi,\pi]^D} e^{i<\lambda,\Sigma\xi_i>} d\lambda$$

After many computations, this leads to the result.