Hadamard Matrices

Peter Sin

University of Florida

UMS. February 22nd, 2022

Definition

A *Hadamard matrix* is an $n \times n$ matrix whose entries are ± 1 that satisfies the equation $H^T H = nI$.

Some examples:

$$\begin{pmatrix} 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}.$$

Definition

A *Hadamard matrix* is an $n \times n$ matrix whose entries are ± 1 that satisfies the equation $H^T H = nI$.

Some examples:

$$(1)\,, \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}.$$

Equivalence: rearrange rows or columns, multiply row or column by -1.

Jacques Hadamard 1865-1963

Hadamard, J. (1893). “Résolution d’une question relative aux déterminants”. Bulletin des Sciences Mathématiques. 17: 240-246.

Hadamard's Inequality

Theorem

Let $X = (x_{ij})$ be an $n \times n$ real matrix with $|x_{ij}| \leq 1$ for all i and j. Then $|\det(X)| \leq n^{n/2}$. Equality holds if and only if X is a Hadamard matrix.

Hadamard Conjecture

Theorem

If a Hadamard matrix of order n exists, then $n = 1$ or 2 or a multiple of 4.

Hadamard Conjecture

Theorem

If a Hadamard matrix of order n exists, then $n = 1$ or 2 or a multiple of 4.

$$
\begin{array}{cccc}
+\cdots+ & +\cdots+ & +\cdots+ & +\cdots+ \\
+\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\
+\cdots+ & -\cdots- & +\cdots+ & -\cdots-
\end{array}
$$

Hadamard Conjecture

Theorem

If a Hadamard matrix of order n exists, then $n = 1$ or 2 or a multiple of 4.

$$
\begin{array}{cccc}
\overbrace{+\cdots+}^{a} & \overbrace{+\cdots+}^{b} & \overbrace{+\cdots+}^{c} & \overbrace{+\cdots+}^{d} \\
+\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\
+\cdots+ & -\cdots- & +\cdots+ & -\cdots-
\end{array}
$$

$$
\begin{cases}
a+b+c+d=n \\
a+b-c-d=0 \\
a-b+c-d=0 \\
a+b-c+d=0
\end{cases}
\qquad \therefore n = 4a.
$$

Hadamard Conjecture

Theorem

If a Hadamard matrix of order n exists, then $n = 1$ or 2 or a multiple of 4.

$$
\begin{array}{cccc}
\overbrace{+\cdots+}^{a} & \overbrace{+\cdots+}^{b} & \overbrace{+\cdots+}^{c} & \overbrace{+\cdots+}^{d} \\
+\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\
+\cdots+ & -\cdots- & +\cdots+ & -\cdots-
\end{array}
$$

$$
\begin{cases}
a+b+c+d = n \\
a+b-c-d = 0 \\
a-b+c-d = 0 \\
a+b-c+d = 0
\end{cases}
\qquad \therefore n = 4a.
$$

Hadamard Conjecture: There exists a Hadamard matrix of order n whenever n is multiple of 4.

Hadamard Conjecture

Theorem

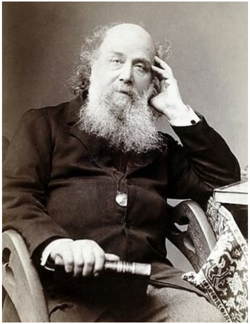
If a Hadamard matrix of order n exists, then $n = 1$ or 2 or a multiple of 4.

$$
\begin{array}{cccc}
\overbrace{+\cdots+}^{a} & \overbrace{+\cdots+}^{b} & \overbrace{+\cdots+}^{c} & \overbrace{+\cdots+}^{d} \\
+\cdots+ & +\cdots+ & -\cdots- & -\cdots- \\
+\cdots+ & -\cdots- & +\cdots+ & -\cdots-
\end{array}
$$

$$
\begin{cases}
a+b+c+d=n \\
a+b-c-d=0 \\
a-b+c-d=0 \\
a+b-c+d=0
\end{cases}
\qquad \therefore n = 4a.
$$

Hadamard Conjecture: There exists a Hadamard matrix of order n whenever n is multiple of 4. Smallest open case is $n = 668$.

Sylvester's Construction



James Sylvester 1814-1897

J.J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. Philosophical Magazine, 34:461-475, 1867

Sylvester's Construction

If A is an $n \times n$ matrix and B is an $m \times m$ matrix, their *Kronecker product* is the $nm \times nm$ matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix}$$

Lemma

The Kronecker product of two Hadamard matrices is a Hadamard matrix.

Thus there are Hadamard matrices of order 2^m for all m.

Paley's constructions

Raymond Paley 1907-1933

Paley, R. E. A. C. (1933). "On orthogonal matrices". Journal of Mathematics and Physics. 12 (1-4): 311-320

Quadratic character

Let $\mathbb{F}_q$ be a finite field of order q (odd prime power). The quadratic character $\chi : \mathbb{F}_q \to \{-1, 0, 1\}$,

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0; \\ 1 & \text{if } a \text{ is a nonzero square;} \\ -1 & \text{if } a \text{ is a nonsquare.} \end{cases}$$

Jacobsthal matrix Q

Q is indexed by $\mathbf{F}_q$, $Q_{a,b} := \chi(a-b)$

Lemma

$QQ^T = qI - J$, where J is the matrix of all ones.

$$(QQ^T)_{aa} = \sum_{b \in \mathbb{F}_q} \chi(a-b)^2 = q - 1.$$

If $c \neq a$,

$$\begin{aligned}(QQ^T)_{ac} &= \sum_{b \in \mathbb{F}_q} \chi(a-b)\chi(c-b) = \sum_{u \in \mathbb{F}_q^\times} \chi(u)\chi(u + (c-a)) \\ &= \sum_{u \in \mathbb{F}_q^\times} \chi(u)^2 \chi(1 + \frac{(c-a)}{u}) = \sum_{u \in \mathbb{F}_q^\times} \chi(1 + \frac{(c-a)}{u}) \\ &= \sum_{\substack{x \in \mathbb{F}_q^\times \\ x \neq 1}} \chi(x) = -1\end{aligned}$$

Paley's First Construction

Assume $q \equiv 3 \pmod 4$. Then -1 is not a square and $Q^T = -Q$.

$$H = I_{q+1} + \left[\begin{array}{c:c} 0 & 1 \cdots 1 \\ \hdashline -1 & \\ \vdots & Q \\ -1 & \end{array}\right]$$

$q = 7$

$$
H = \begin{array}{c} \\ \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array}
\begin{array}{c} \begin{array}{cccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\
\left(\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
-1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\
-1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
-1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & 1
\end{array}\right) \end{array}
$$

Paley's Second Construction

Assume $q \equiv 1 \pmod 4$. Then -1 is a square and $Q^T = Q$.

$$C = \left[\begin{array}{c:c} 0 & 1 \cdots 1 \\ \hdashline 1 & \\ \vdots & Q \\ 1 & \end{array}\right]$$

$$H = \left[\begin{array}{c:c} C + I_{q+1} & C - I_{q+1} \\ \hdashline C - I_{q+1} & -C - I_{q+1} \end{array}\right]$$

Skew and Symmetric Hadamard Matrices

A Hadamard matrix is *symmetric* of $H = H^T$ and is *skew* if $H - I_n$ is skew-symmetric, i.e. $H + H^T = 2I$. Paley's first construction gives skew Hadamard matrices and the second construction gives symmetric ones.

Skew and Symmetric Hadamard Matrices

A Hadamard matrix is *symmetric* of $H = H^T$ and is *skew* if $H - I_n$ is skew-symmetric, i.e. $H + H^T = 2I$. Paley's first construction gives skew Hadamard matrices and the second construction gives symmetric ones. Conjectures: There is a skew (resp. symmetric) Hadamard matrix of order equal to any multiple of 4.

Skew and Symmetric Hadamard Matrices

A Hadamard matrix is *symmetric* of $H = H^T$ and is *skew* if $H - I_n$ is skew-symmetric, i.e. $H + H^T = 2I$. Paley's first construction gives skew Hadamard matrices and the second construction gives symmetric ones. Conjectures: There is a skew (resp. symmetric) Hadamard matrix of order equal to any multiple of 4. Smallest open case is $n = 276$ for skew, $n = 188$ for symmetric.

Circulant Hadamard Matrices

A *circulant* matrix is one where each row is a cyclic shift of the previous row:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}$$

An example of a circulant Hadamard matrix is

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

Circulant Hadamard Matrices

A *circulant* matrix is one where each row is a cyclic shift of the previous row:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}$$

An example of a circulant Hadamard matrix is

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

Conjecture: The only possible orders of a circulant Hadamard matrix are 1 and 4.

Circulant Hadamard Matrices

A *circulant* matrix is one where each row is a cyclic shift of the previous row:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}$$

An example of a circulant Hadamard matrix is

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

Conjecture: The only possible orders of a circulant Hadamard matrix are 1 and 4. Popular problem, many incorrect proofs.

Complex Hadamard Matrices

Generalize to complex matrices.

$$|H_{ij}| = 1, \qquad HH^* = nI.$$

An important example is the Fourier matrix $F(n)$:
$F(n)_{rs} = \omega^{(r-1)(s-1)}$, $\omega = e^{\frac{2\pi i}{n}}$.

$$F(5) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega^1 & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

So complex Hadamard matrices of all orders exist.

Explore further

I just scratched the surface. There is a vast literature on Hadamard matrices and their applications such as in error correcting codes (Hadamard codes), telecommunications (CDMA Walsh codes), statistics (Plackett-Burman designs). The topic is still very active after 150 years.

$$\begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}$$

$$\begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&1&1\\ 0&1&1&0&0&1&1&0\\ 0&0&0&0&1&1&1&1\\ 0&1&0&1&1&0&1&0\\ 0&0&1&1&1&1&0&0\\ 0&1&1&0&1&0&0&1\\ 1&1&1&1&1&1&1&1\\ 1&0&1&0&1&0&1&0\\ 1&1&0&0&1&1&0&0\\ 1&0&0&1&1&0&0&1\\ 1&1&1&1&0&0&0&0\\ 1&0&1&0&0&1&0&1\\ 1&1&0&0&0&0&1&1\\ 1&0&0&1&0&1&1&0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$