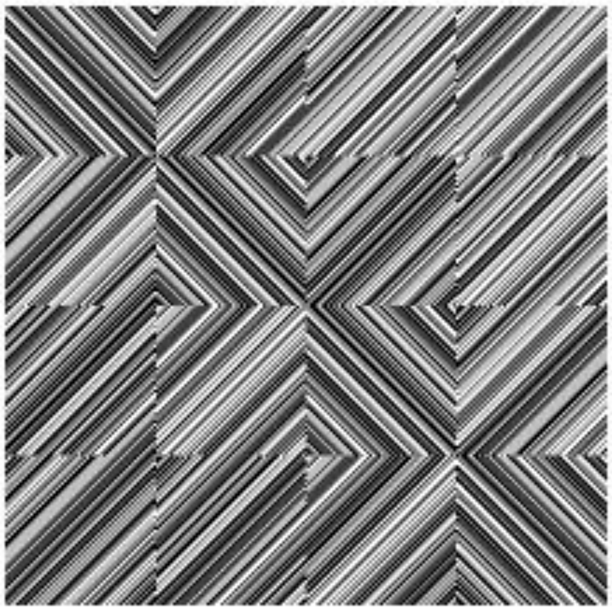
An Introduction to Hadamard Matrices, their Constructions, and Generalizations



Charles Katerba

Arizona Space Grant Symposium

April 17, 2010

NORTHERN ARIZONA UNIVERSITY

What is a Hadamard Matrix?

In the 1890's, *J. Hadamard* asked this question:

"What $n \times n$ matrices with entries from the set $\{\pm 1\}$ have maximal determinants?"

An $n \times n$ matrix H with the above properties is now called a *Hadamard matrix*. It follows that an $n \times n$ *HM* has the following characteristics**:**

- H must satisfy $H \cdot H^T = n \cdot I_n$
- the rows (and columns) must be pairwise orthogonal
- n must be a multiple of 4 (or $n = 1 \text{ or } 2$)
- rows and columns are *pairwise balanced*

Where Do They Come From?

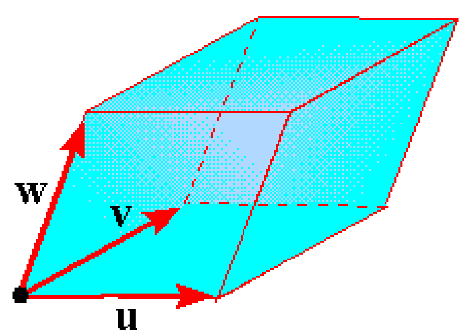
The Hadamard Inequality: Let M be a square matrix of order n. Then

$$|\det(M)| \le n^{n/2}$$

This bound is achieved when $M \cdot M^T = n \cdot I_n$

$$(\det(M))^2 = \det(M) \cdot \det(M) = \det(M) \cdot \det(M^T)$$
$$= \det(M \cdot M^T) = \det(n \cdot I_n) = n^n$$
$$\Rightarrow \det(M) = n^{n/2}$$

Orthogonality:



Vs.

Example: Here, H is a symmetric matrix, but only to make the computations easy.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad H^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$H \cdot H^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4 \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = 4 \cdot I_4$$

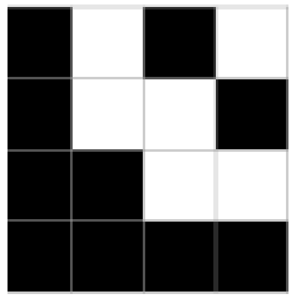
<u>**Applications of Hadamard Matrices**</u>

- Finding Errors in Coding Theory
- Cryptography
- Measuring variability in stratified sampling
- Buffering in spectroscopic analysis
- Signal modulation
- Separation of electronic transmissions
- Improving signal correlation
- Enhancing 3-D optical memory storage
- Quantum Mechanics

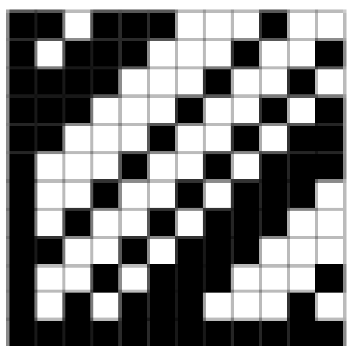
So knowing when a *HM* exists, and of what orders they exist, is important.

Classic Constructions

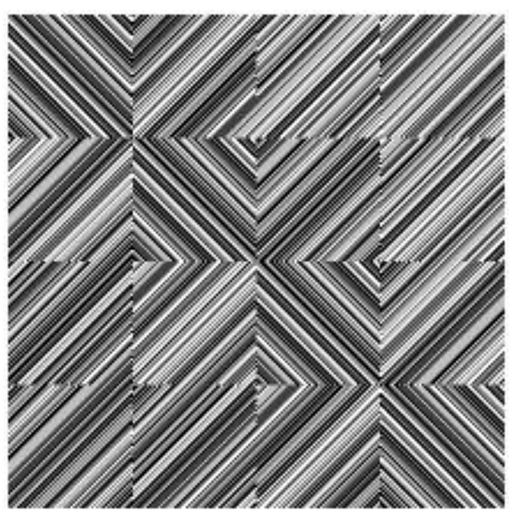
- Sylvester Construction (matrix tensor products)



- Payley Construction (quadratic group characters)



- Williamson Construction (Plug-in technique)



Hadamard Matrix Generalizations

Butson Hadamard Matrices: Let H be an $n \times n$ matrix whose entries are complex m^{th} roots of unity instead of $\{\pm 1\}$.

Unimodular HMs: Let H be an $n \times n$ matrix with entries come the complex unit circle in place of complex m^{th}roots of unity.

Generalized HMs: Let H be an $n \times n$ matrix whose entries come from any finite group instead of the complex unit circle.

Higher Dimensional HMs: Let H be an $n \times n \times ... \times n$ array with entries from the set $\{\pm 1\}$.

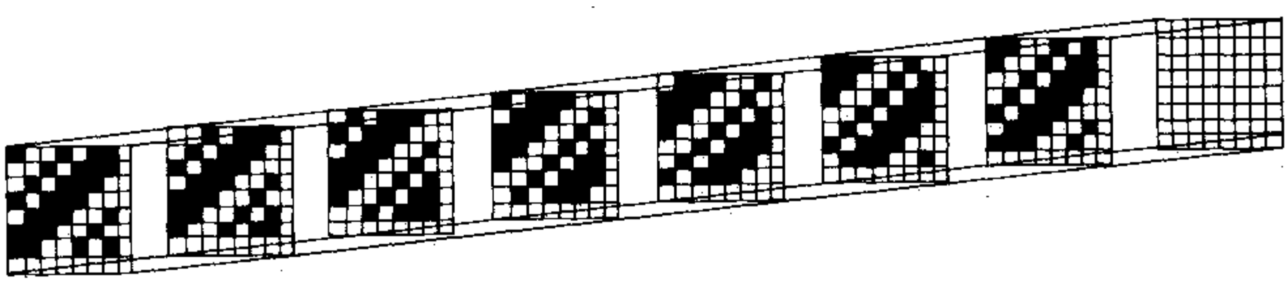


Fig. 2. Paley cube of dimension 3, ■ Minus one. □ Plus one.

Circulant Hadamard Conjecture

Definition: A *circulant matrix* is defined by its first row. For each subsequent row, take each entry from the first row and move it down one row and to the right one entry.

Example:

$$\begin{bmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$$, which is Hadamard.

Circulant Hadamard Conjecture: There are no circulant Hadamard matrices of order > 4.

John's Work: The only possible orders of circulant Hadamard matrices are of the form

$$4u^2, \text{ where } u \text{ is odd}.$$

Acknowledgements

- The NASA Space Grant Program at NAU
- The NAU Department of Mathematics and Statistics
- The Office of the Vice President for Research and Development at NAU
- Jeff Rushall
- Dr. Jennifer Seberry, *Hadamard Queen*

NORTHERN
ARIZONA
UNIVERSITY