Hadamard matrices

Monika Seidlová

Spring school of algebra

March 24, 2012

Hadamard matrices

Introduction

- Orders and the Hadamard conjecture
- Sylvester's construction
- Paley's construction
- Williamson's construction

Hadamard matrices

Definition: An $(n \times n)$ matrix $\mathbf{H}$ with entries 1 or -1, such that $\mathbf{H} \cdot \mathbf{H}^T = n\mathbf{I}_n$, is called an *Hadamard matrix of order n*.
If $\mathbf{H}$ is Hadamard's, then

$$\mathbf{H} \cdot \mathbf{H}^T = n\mathbf{I}_n \tag{1}$$

$$\mathbf{H}^T \cdot \mathbf{H} = n\mathbf{I}_n \tag{2}$$

Therefore, each two distinct rows as well as columns differ in exactly half the entries. In other words, any two distinct rows or columns are orthogonal.

Hadamard matrices

Examples of small Hadamard matrices:

$$\mathbf{H_1} = (1)$$

$$\mathbf{H_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

Hadamard matrices

Definition: We say an Hadamard matrix is *normalized* if the first row and first column contain only 1s.

Definition: Two Hadamard matrices are said to be *equivalent* if one can be obtained from the other by negating rows or columns, or by interchanging rows or columns.

Every Hadamard matrix is equivalent to a normalized one.

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

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

Hadamard matrices

Theorem: If an Hadamard matrix of order n exists for a given $n \geq 1$, then $n = 1$, 2 or n is a multiple of 4.
Proof: Let $n > 2$ and $\mathbf{H}$ be a normalized Hadamard matrix of order n. Put
A := { j | the entry in the 2^{nd} row, j^{th} column is 1}
B := { j | the entry in the 3^{nd} row, j^{th} column is 1}
|A| = # 1s in 2^{nd} row
|B| = # 1s in 3^{rd} row
|A| = |B| = $n/2$
The 2^{nd} and 3^{rd} rows differ in $|A| + |B| - 2|A \cap B|$ entries.

$$n/2 = |A| + |B| - 2|A \cap B| \tag{3}$$
$$n/2 = n/2 + n/2 - 2|A \cap B| \tag{4}$$
$$|A \cap B| = n/4 \tag{5}$$

Therefore, n is a multiple of 4.

Hadamard matrices

The previous theorem leads up to the **Hadamard Conjecture**:

For every k natural, an Hadamard matrix of order 4k exists.

The smallest multiple of 4, of which order no Hadamard matrix is presently known, is 668.

Hadamard matrices

Kronecker product

Definition: Given an $(m \times n)$ matrix $\mathbf{A}$ and a $(p \times q)$ matrix $\mathbf{B}$, their *Kronecker product* $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$ is an $(mp \times nq)$ matrix with elements defined by $c_{\alpha\beta} = a_{ij} b_{kl}$, where
$\alpha = p(i-1) + k$
$\beta = q(j-1) + l$

For example, the Kronecker product of the (2×2) matrix $\mathbf{A}$ and the (3×2) matrix $\mathbf{B}$ is shown in the following (6×4) matrix

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{11}b_{31} & a_{11}b_{32} & a_{12}b_{31} & a_{12}b_{32} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \\ a_{21}b_{31} & a_{21}b_{32} & a_{22}b_{31} & a_{22}b_{32} \end{pmatrix}$$

Hadamard matrices

Sylvester's construction

In 1867, James Sylvester was the first one to write about what we now call Hadamard matrices. He described a construction of these matrices.

Theorem: If $\mathbf{H}$ is an Hadamard matrix of order n, then

$$\mathbf{H}' = \begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$$

is an Hadamard matrix of order $2n$.

Since $\mathbf{H_1} = (1)$ is an Hadamard matrix of order 1, the following Corollary flows from Sylvester's construction:
There is an Hadamard matrix of order 2^t for all natural t.

Hadamard matrices

Sylvester's construction

Theorem (Sylvester): Let $\mathbf{H_{n_1}}$ and $\mathbf{H_{n_2}}$ be Hadamard matrices of orders n_1 and n_2, then the Kronecker product of $\mathbf{H_{n_1}}$ and $\mathbf{H_{n_2}}$ is an Hadamard matrix of order $n_1 n_2$.

Sylvester's construction can be formalized using the matrix

$$\mathbf{H_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Then we have that

$$\mathbf{H_{2^t}} = \begin{pmatrix} \mathbf{H_{2^{t-1}}} & \mathbf{H_{2^{t-1}}} \\ \mathbf{H_{2^{t-1}}} & -\mathbf{H_{2^{t-1}}} \end{pmatrix} = \mathbf{H_2} \otimes \mathbf{H_{2^{t-1}}},$$

for $2 \leq t \in N$.

Hadamard matrices

Paley's construction

Definition: Let q be an odd prime power. The quadratic character χ on the group F_q is defined as follows

$$\chi(g) = \begin{cases} 1 & \text{if } g \text{ is a quadratic residue in } F_q \\ -1 & \text{if } g \text{ is a quadratic nonresidue in } F_q \\ 0 & \text{if } g = 0. \end{cases}$$

Hadamard matrices

Paley's construction

Theorem: For q an odd prime power and an ordering $\{g_0 = 0, g_1, \ldots, g_{q-1}\}$ of F_q, set $\mathbf{Q} = (\chi(g_i - g_j))_{0 \le i,j < q}$. Let $\mathbf{S}$ be the $((q+1) \times (q+1))$ matrix

$$\mathbf{S} = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^T & \mathbf{Q} \end{pmatrix}, \text{ where } \mathbf{1} \text{ is a vector of 1s.}$$

If $q \equiv 3 \bmod 4$, then

$$\mathbf{P_q} = \begin{pmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^T & \mathbf{Q} + \mathbf{I_q} \end{pmatrix} \text{ is an Hadamard matrix of order } (q+1).$$

If $q \equiv 1 \bmod 4$, then

$$\mathbf{P'_q} = \begin{pmatrix} \mathbf{S} + \mathbf{I_{q+1}} & \mathbf{S} - \mathbf{I_{q+1}} \\ \mathbf{S} - \mathbf{I_{q+1}} & -\mathbf{S} - \mathbf{I_{q+1}} \end{pmatrix}$$

is an Hadamard matrix of order $2(q+1)$.

Hadamard matrices

Example of Paley's construction

For $q = 3$, we have $F_3 = \{0, 1, 2\}$. 1 is a quadratic residue, 2 is a quadratic nonresidue. We have that

$\chi(0) = 0$

$\chi(1) = 1$

$\chi(2) = -1$

We construct $\mathbf{Q} = (\chi(i-j))_{0 \leq i,j < 3}$

$$\mathbf{Q} = \begin{pmatrix} \chi(0) & \chi(2) & \chi(1) \\ \chi(1) & \chi(0) & \chi(2) \\ \chi(2) & \chi(1) & \chi(0) \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$$

$3 \equiv 3 \bmod 4$, so we construct an Hadamard matrix of order 4.

$$\mathbf{P_3} = \begin{pmatrix} 1 & -\mathbf{1} \\ \mathbf{1}^T & \mathbf{Q} + \mathbf{I_3} \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix}$$

Hadamard matrices

Paley's construction

Definition: Let $\{q_i, i \in I\}$ and $\{q'_j, j \in J\}$ be finite sets of prime powers congruent to 3 mod 4 and 1 mod 4, respectively. A matrix of the form

$$(\otimes_{i\in I} \mathbf{P_{q_i}}) \otimes (\otimes_{j\in J} \mathbf{P'_{q'_j}}),$$

which is an Hadamard matrix of order $\prod_{i\in I}(q_i+1)\prod_{j\in J} 2(q'_j+1)$, is called a *Paley Hadamard matrix*.

Hadamard matrices

Equivalence

Are the matrices

$$\mathbf{P_3} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix} \text{ and } \mathbf{H_4} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

which we get from Sylvester's construction from $\mathbf{H_1} = (1)$, equivalent?

Do different constructions yield inequivalent Hadamard matrices?

Hadamard matrices

Equivalence

$$\mathbf{P_3} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

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

Hadamard matrices

Equivalence

$\mathbf{P_3}$ and $\mathbf{H_4}$ must be equivalent, because there is only one class of equivalence for Hadamard matrices of order 4.

order	1	2	4	8	12	16	20	24	28	2^n
# of classes	1	1	1	1	1	5	3	60	487	$\geq 10 \left\lfloor \frac{n}{5} \right\rfloor + 1$

The smallest order that cannot be constructed by a combination of Sylvester's and Paley's methods is 92. The following construction was used in 1962 to construct $\mathbf{H_{92}}$ by a computer.

Hadamard matrices

Williamson's construction

Theorem: Suppose there exist four symmetric matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ of order n with entries 1 and -1 which satisfy

$$\mathbf{X}\mathbf{Y}^T = \mathbf{Y}\mathbf{X}^T, \forall\, \mathbf{X}, \mathbf{Y} \in \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}\}.$$

Further, suppose

$$\mathbf{A}\mathbf{A}^T + \mathbf{B}\mathbf{B}^T + \mathbf{C}\mathbf{C}^T + \mathbf{D}\mathbf{D}^T = 4n\mathbf{I_n}.$$

Then, using $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ in the Williamson array $\mathbf{H}$ given by

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

gives an Hadamard matrix of order $4n$.

Hadamard matrices

Example of Williamson's construction

$$\text{Let } \mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \mathbf{B} = \mathbf{C} = \mathbf{D} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$$

$$\mathbf{A^2} = \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix}, \mathbf{B^2} = \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}$$

Thus, $\mathbf{AA}^T + \mathbf{BB}^T + \mathbf{CC}^T + \mathbf{DD}^T = 4n\mathbf{I_n}$. We can use matrices $\mathbf{A}$ and $\mathbf{B}$ to construct an Hadamard matrix of order 12.

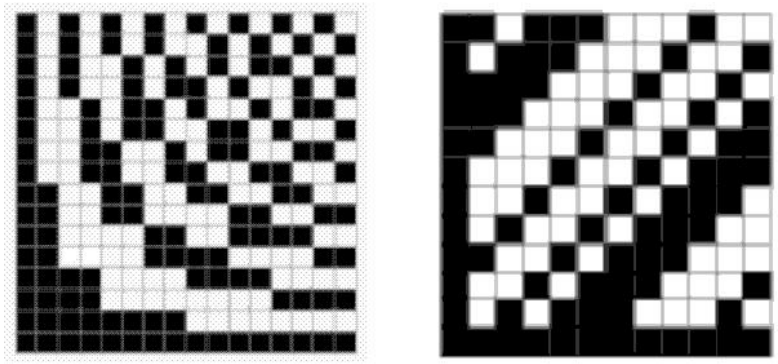
Hadamard matrices

Example of Williamson's construction

$$\mathbf{H_{12}} = \left(\begin{array}{ccc|ccc|ccc|ccc}
+ & + & + & - & + & + & - & + & + & - & + & + \\
+ & + & + & + & - & + & + & - & + & + & - & + \\
+ & + & + & + & + & - & + & + & - & + & + & - \\
\hline
+ & - & - & + & + & + & + & - & - & - & + & + \\
- & + & - & + & + & + & - & + & - & + & - & + \\
- & - & + & + & + & + & - & - & + & + & + & - \\
\hline
+ & - & - & - & + & + & + & + & + & + & - & - \\
- & + & - & + & - & + & + & + & + & - & + & - \\
- & - & + & + & + & - & + & + & + & - & - & + \\
\hline
+ & - & - & + & - & - & - & + & + & + & + & + \\
- & + & - & - & + & - & + & - & + & + & + & + \\
- & - & + & - & - & + & + & + & - & + & + & +
\end{array}\right)$$

Hadamard matrices

Conclusion



- Orders and the Hadamard conjecture
- Sylvester's construction
- Paley's construction
- Williamson's construction