Hadamard matrices

A Hadamard matrix of order $n$ is a matrix of type $n \times n$ whose coefficients are $1$ or $-1$ and such that

$$HH^T = nI_n.$$  

Note that this relation is equivalent to say that the rows of $H$ have norm $\sqrt{n}$ and that any two distinct rows are orthogonal. Since $H$ is invertible and $H^T = nH^{-1}$, we see that

$$H^TH = nH^{-1}H = nI_n$$
and hence $H^T$ is also a Hadamard matrix. Thus $H$ is a Hadamard matrix if and only if its columns have norm $\sqrt{n}$ and any two distinct columns are orthogonal.

- If $H$ is a Hadamard matrix of order $n$, then
  $$\det(H) = \pm n^{n/2}.$$  

In particular we see that the Hadamard matrices satisfy the equality in Hadamard's inequality:

$$|\det(A)| \leq \prod_{i=1}^{n} (\sum_{j=1}^{n} a_{ij}^2)^{1/2},$$

which is valid for all real matrices $A = (a_{ij})$ of order $n$.

**Remark.** The expression $n^{n/2}$ is the supremum of the value of $\det(A)$ when $A$ runs over the real matrices such that $|a_{ij}| \leq 1$. Moreover, the equality is reached if and only if $A$ is a Hadamard matrix.
If we change the signs of a row (column) of a Hadamard matrix, the result is clearly a Hadamard matrix.

If we permute the rows (columns) of a Hadamard matrix, the result is another Hadamard matrix.

Two Hadamard matrices are called equivalent (or isomorphic) if it is to go from one to the other by means of a sequence of such operations. Observe that by changing the sign of all the columns that begin with $-1$, and afterwards all the rows that begin with $-1$, we obtain an equivalent Hadamard matrix whose first row and first column only contain $+1$. Of such matrices we say that are normalized Hadamard matrices.

**Example.** \( H^{(1)} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \) is the unique normalized Hadamard matrix of order 2. More generally, if we define \( H^{(n)} \), \( n \geq 2 \), recursively by the formula
\[ H^{(n)} = \begin{pmatrix} H^{(n-1)} & H^{(n-1)} \\ H^{(n-1)} & -H^{(n-1)} \end{pmatrix}, \]

then \( H^{(n)} \) is a normalized Hadamard matrix of order \( 2^n \).

It is also easy to check that if \( H \) and \( H' \) are Hadamard matrices of orders \( n \) and \( n' \), then the tensor product \( H \otimes H' \) is a Hadamard matrix of order \( nn' \) (the matrix \( H \otimes H' \), also called the Kronecker product of \( H \) and \( H' \), can be defined as the matrix obtained by substituting each component \( a_{ij} \) of \( H \) by the matrix \( a_{ij}H' \)). For example, if \( H \) is a Hadamard matrix of order \( n \), then

\[ H^{(1)} \otimes H = \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \]

is a Hadamard matrix of order \( 2n \). Notice also that

\[ H^{(n)} = H^{(1)} \otimes H^{(n-1)}. \]
**Proposition.** If $H$ is a Hadamard matrix of order $n \geq 3$, then $n$ is divisible by 4.

**Remark.** Any two Hadamard matrices of order 4 are equivalent.

\[
\begin{pmatrix}
+ & + & + & + \\
+ & + & - & - \\
+ & - & + & - \\
+ & - & - & + \\
\end{pmatrix}.
\]

The same happens for order 8, but later on we will see that this is no longer the case for order 12.

**The Paley construction of Hadamard matrices**

Suppose that the cardinal of $F$, $q$, is odd, so that $q = p^r$ with $p > 2$, $p$ prime. Let

\[\chi: F^* \to \{\pm 1\}\]
be the *Legendre character* of $F^*$, namely

$$\chi(x) = x^{(q-1)/2} = \begin{cases} 1 & \text{if } x \text{ is a square (quadratic residue)} \\ -1 & \text{if } x \text{ is not a square} \end{cases}$$

(conventionally we define $\chi(0) = 0$). Note that $\sum_{x \in F} \chi(x) = 0$.

If we enumerate the elements of $F$ (in some order),

$$x_0 = 0, x_1, \ldots, x_{q-1},$$

the *Paley matrix* of $F$,

$$S_q = (s_{ij}) \in M_q(F),$$

is defined by the formula

$$s_{ij} = \chi(x_i - x_j).$$
**Proposition.** If $U = U_q \in M_q(F)$ is the matrix with all its entries equal to 1, then $S = S_q$ has the following properties:

1) $S 1_q^T = 0_q^T$

2) $1_q S = 0_q$

3) $SS^T = q I_q - U$

4) $S^T = (-1)^{(q-1)/2} S$. 
Theorem. If $n = q + 1 \equiv 0 \mod 4$, then the matrix

$$H_n = \begin{pmatrix} 1 & 1_q \\ 1_q^T & -I_q \pm S_q \end{pmatrix}$$

is a Hadamard matrix of order $n$. It is called the Hadamard matrix of $F$.

In the case that $q + 1$ is not divisible by 4, it is possible to construct a Hadamard matrix of order $2q + 2$, as we will see in the exercises.

We are going to use the following concept: a matrix $C$ of order $n > 1$ is a conference matrix if its principal diagonal is zero, the other elements are $\pm 1$ and $CC^T = (n - 1)I_n$. It is immediate to check that the order of a conference matrix is necessarily even.

---

1 The first ten $q$ that satisfy this condition are 7, 11, 19, 23, 27, 31, 37, 43, 47, 59.
Remark. Let $S$ be the Paley matrix of a finite field $F = \mathbb{F}_q$, $q$ odd, and let $\varepsilon = 1$ if $S$ is symmetric and $\varepsilon = -1$ if $S$ is skew-symmetric. Then

$$C = \begin{pmatrix} 0 & 1_q \\ \varepsilon 1_q^T & S \end{pmatrix}$$

is a conference matrix of order $q + 1$ (it is called the conference matrix of $F$). This matrix is symmetric if $q \equiv 1 \mod 4$ and skew-symmetric if $q \equiv 3 \mod 4$. Note that in the case $q \equiv 3 \mod 4$ the matrix $I_n + C$ is equivalent to the matrix $H_n$ of the previous theorem.

Remark. a) If $C$ is an skew-symmetric conference matrix of order $n$, $H = I_n + C$ is a Hadamard matrix.

b) If $C$ is a symmetric conference matrix of order $n$,

$$\bar{H} = \begin{pmatrix} I_n + C & -I_n + C \\ -I_n + C & -I_n - C \end{pmatrix}$$

is a Hadamard matrix of order $2n$. 
c) If $C$ is the conference matrix of a finite field $F = \mathbb{F}_q$, and $q + 1$ is divisible by 4, (b) yields a Hadamard matrix of order $2q + 2$. This matrix will be called the *Hadamard matrix de $F$*. 

**Remark.** The Hadamard matrices $H^{(2)}, H^{(3)}, H^{(4)}, H^{(5)}$ have order 4, 8, 16, 32. For $q = 7, 11, 19, 23, 27, 31$, the theorem yields Hadamard matrices $H_8, H_{12}, H_{20}, H_{24}, H_{28}, H_{32}$. Part (c) of the preceding remark, applied to the fields $\mathbb{F}_5, \mathbb{F}_9$ and $\mathbb{F}_{13}$, provides us with matrices $\overline{H}_{12}, \overline{H}_{20}, \overline{H}_{28}$.

Thus we have Hadamard matrices of orders 4, 8, 12, 16, 20, 24, 28 and 32. Proceeding in similar ways, and with others that are beyond the scope of these notes, we can construct Hadamard matrices for many orders. The first ordre $n$ for which no Hadamard matrix is known is $n=668$ (the previous value was 428, but it was solved by Behruz Tayfeh-Rezaie in 2004).
Is is conjectured that for any $n$ that is multiple of 4 there is a Hadamard matrix of order $n$. This is usually called the Hadamard conjecture, but it is probably due to Raymond Paley (1993).

**Remark.** The matrices $H^{(3)}$ and $H_8$ are distinct, but they are equivalent (all the Hadamard matrices of order 8 are equivalent). It can also be seen that the matrices $H_{12}$ and $\overline{H}_{12}$ are equivalent, even though it turns out that there are Hadamard matrices of order 12 that are not equivalent.
**Code associated to a Hadamard matrix**

We associate a code $C = C_H$ of type $(n, 2n)$ to any Hadamard matrix $H$ of order $n$ as follows:

$$C = C' \cup C''$$

where $C'$ ($C''$) is the $n \times n$ binary matrix obtained by the substitution $-1 \rightarrow 0$ in $H$ ($-H$). Notice that the words in $C''$ can also be obtain as the complements of the words in $C'$.

Since two rows of $H$ differ in exactly $n/2$ positions, the minimum distance of $C_H$ is $n/2$. Hence $C_H$ is a code of type $(n, 2n, n/2)$. In general this code is not linear (a necessary condition for linearity is that $n$ be a power of 2).

Note that $C_H$ is not equidistant, as it contains the words $1_n$ and $0_n$. 
Example. The code $C_{H_8}$ is equivalent to the parity completion of the Hamming code $[7,4,3]$. In particular, it is a linear code.

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
\end{pmatrix}
\]

$1 + 2 + 3 + 4$

$1 + 3 + 4$

$1 + 4$

$1$

$1 + 2$

$1 + 3$

$1 + 2 + 4$

$1 + 2 + 3$

$0$

$2$

$2 + 3$

$2 + 3 + 4$

$3 + 4$

$2 + 4$

$3$

$4$
**Example.** The code $C = C_{H}^{(5)} \sim (32,64,16)$ is the code used in the period 1969-1972 by the Mariner spacecraft to transmit images of Mars (this code also turns out to be linear, and actually equivalent to lineal $RM_{2}(5)$).

**Decoding Hadamard codes**

Let $C = C_{H}$ be the Hadamard code associated to the Hadamard matrix $H$. Let $n$ be the order of $H$ and

$$t = \lfloor (n/2 - 1)/2 \rfloor = \lfloor (n - 2)/4 \rfloor = (n - 4)/4$$

its error-correcting capacity $C$.

Given a vector $y$ of length $n$, let $\hat{y} \in \{1, -1\}^{n}$ be the result of performing the substitution $0 \to -1$ in $y$. For example, from the definition of $C$ it turns out that if $x \in C'$ (or $x \in C''$), then $\hat{x}$ (or $-\hat{x}$) is a row of $H$. 
**Lemma.** Let $y$ be a binary vector of length $n$, $z$ the result of negating an entry of $y$, and $h$ any row of $H$. Then

$$\langle \hat{z}|h\rangle = \langle \hat{y}|h\rangle \pm 2.$$ 

**Proposition.** Let $C = C_H$, where $H$ is a Hadamard matrix of order $n$. Suppose that $x \in C$ is the sent vector, that $e$ is the error vector and that $y = x + e$ is the received vector. Let $s = |e|$ and suppose that $s \leq t$. Then there is a unique row $h = h_y$ of $H$ such that

$$|\langle \hat{y}|h\rangle| > n/2 \text{ and } |\langle \hat{y}|h'\rangle| < n/2 \text{ for all other rows } h' \text{ of } H.$$ 

Moreover, $\hat{x} = h$ or $\hat{x} = -h$ according to whether $\langle \hat{y}|h\rangle > 0$ or $\langle \hat{y}|h\rangle < 0$. 
Decoding algorithm

Input: \( y \) (the received vector).

1) Calculate \( \hat{y} \).

2) Calculate \( c = \langle \hat{y}|h \rangle \) for the successive rows \( h \) of \( H \), and stop as soon as \( |c| > n/2 \) or if there are no more rows. In this second case return Error.

3) Return the result of performing the substitution \(-1 \rightarrow 0\) in the vector \( h \)\((-h)\) if \( c > 0 \) \((c < 0)\).

Exercise. The code \( RM_2(m) \) is equivalent to the Hadamard code \( C_{H(m)} \).

Hint: If \( H \) is a control matrix of \( \text{Ham}_2(m) \), then the matrix

\[
\tilde{H} = \begin{pmatrix} 1 & 1_{2^m-1} \\ 0_m^T & H \end{pmatrix}
\]

is a generating matrix of \( RM_2(m) \).