10 Hadamard Matrices

Hadamard Matrix: An $n \times n$ matrix $H$ with all entries $\pm 1$ and $HH^\top = nI$ is called a Hadamard matrix of order $n$. For brevity, we use $+$ instead of 1 and $-$ instead of $-1$.

Examples:

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

Notes: If two matrices have product $tI$ then they commute. It follows that $H^\top H = nI$ for every Hadamard matrix of order $n$. Also note that modifying a Hadamard matrix by multiplying a row/column by -1 or permuting the rows/columns yields another Hadamard matrix.

Observation 10.1 If $H$ is a Hadamard matrix of order $n$ then $n = 1, 2$ or $n \equiv 0 \pmod{4}$.

Proof: We may assume $n \geq 3$ and may assume (by possibly multiplying columns by $-1$) that the first row has all entries $+$. Now, the first three entries of each column must be $+++, +++-, +++, -$ or $+--$ and we shall assume that there are respectively $a, b, c,$ and $d$ of these. Now we have $a + b + c + d = n$ and the three orthogonality relations on the first three rows yield the equations: $a + b - c - d = 0$, $a + c - b - d = 0$ and $a - b - c + d = 0$. Summing these four equations yields $4a = n$ \qed

Conjecture 10.2 There exists a Hadamard matrix of order $n$ whenever $4$ divides $n$

Tensor Product: Let $A = \{a_{i,j}\}$ be an $m \times n$ matrix and let $B$ be a matrix. Then

$$
A \otimes B = \begin{bmatrix}
a_{1,1}B & a_{1,2}B & \ldots & a_{1,n}B \\
a_{2,1}B & a_{2,2}B & \ldots & a_{2,n}B \\
\vdots & \vdots & & \vdots \\
a_{m,1}B & a_{m,2}B & \ldots & a_{m,n}B
\end{bmatrix}
$$

Note: if $A, B$ have the same dimensions and $C, D$ have the same dimensions, then

$$
(A \otimes C)(B \otimes D) = (AB) \otimes (CD) \quad (1)
$$

$$
(A \otimes C)^\top = A^\top \otimes C^\top \quad (2)
$$
Observation 10.3  If $H_1, H_2$ are Hadamard matrices, then $H_1 \otimes H_2$ is a Hadamard matrix.

Proof: This follows immediately from the above equations. ∎

Character: A character of a (multiplicative) group $G$ is a function $\chi : G \to \mathbb{C}$ which is a group homomorphism between $G$ and the multiplicative group $\{z \in \mathbb{C} : ||z|| = 1\}$. Whenever $q$ is a power of an odd prime, we define $\chi^{\Box} : \mathbb{F}_q \to \mathbb{C}$ as follows

$$\chi^{\Box}(a) = \begin{cases} 
0 & \text{if } a = 0 \\
1 & \text{if } a \in \mathbb{F}_q^{\Box} \\
-1 & \text{otherwise}
\end{cases}$$

Observation 10.4

(i) $\chi^{\Box}(ab) = \chi^{\Box}(a)\chi^{\Box}(b)$ for all $a, b \in \mathbb{F}_q$. (so $\chi^{\Box}$ is a character)

(ii) $\chi^{\Box}(-1) = \begin{cases} 
1 & \text{if } q \equiv 1 \pmod{4} \\
-1 & \text{if } q \equiv 3 \pmod{4}
\end{cases}$.

(iii) $\sum_{a \in \mathbb{F}_q} \chi^{\Box}(a) = 0$

(iv) If $b \in \mathbb{F}_q \setminus \{0\}$ then $\sum_{a \in \mathbb{F}_q} \chi^{\Box}(a)\chi^{\Box}(b + a) = -1$

Proof: The multiplicative group $\mathbb{F}_q \setminus \{0\}$ is cyclic, and thus isomorphic to $\mathbb{Z}_{q-1}$. So, if we choose a generator $g$ for this group we may write its elements as $1 = g^0, g^1, g^2, \ldots, g^{q-2}$. Now, the squares $\mathbb{F}_q^{\Box} = \{g^0, g^2, g^4, \ldots, g^{q-3}\}$ form a (multiplicative) subgroup of index 2. Parts (i) and (iii) follow immediately from this. Since $-1$ is the unique nonidentity element whose square is the identity we have that $-1 = g^{\frac{q-1}{2}}$, so if $q \equiv 1 \pmod{4}$ then $-1 \in \mathbb{F}_q^{\Box}$ and otherwise $-1 \not\in \mathbb{F}_q^{\Box}$ which establishes (ii). For (iv) we have

$$\sum_{a \in \mathbb{F}_q} \chi^{\Box}(a)\chi^{\Box}(b + a) = \sum_{a \in \mathbb{F}_q \setminus \{0\}} (\chi^{\Box}(a))^2 \chi^{\Box}(ba^{-1} + 1)$$

$$= \sum_{c \in \mathbb{F}_q \setminus \{1\}} \chi^{\Box}(c)$$

$$= -1$$

as desired. ∎
Conference Matrix: An $n \times n$ matrix $C$ with all diagonal entries 0 all other entries $\pm 1$ and $CC^T = (n-1)I$ is called a conference matrix.

Lemma 10.5 Let $C$ be a conference matrix.

(i) If $C$ is antisymmetric, then $I + C$ is a Hadamard matrix.

(ii) If $C$ is symmetric, then $I + C - I + C^T - I + C - I - C$ is a Hadamard matrix.

Proof: For (i) we have $(I + C)(I + C)^T = I + C + C^T + CC^T = nI$. Part (ii) is similar. For instance, the upper left submatrix of the product is $(I + C)(I + C)^T + (-I + C)(-I + C)^T = (I + 2C + (n-1)I) + (-I - 2C + (n-1)I) = 2nI$ and the other submatrices are similarly easy to verify. □

Theorem 10.6 Let $q$ be a power of an odd prime. There exists a Hadamard matrix of order $q + 1$ if $q \equiv 3 \pmod{4}$ and a Hadamard matrix of order $2(q + 1)$ if $q \equiv 1 \pmod{4}$.

Proof: Let $a_1, a_2, \ldots, a_q$ be the elements of $\mathbb{F}_q$ and define a matrix $B = \{b_{ij}\}_{1 \leq i, j \leq q}$ by the rule $b_{ij} = \chi(a_i - a_j)$. Now we have

$$(BB^T)_{ij} = \sum_{1 \leq k \leq q} b_{ik}b_{jk}$$

$$= \sum_{1 \leq k \leq q} \chi(a_i - a_k)\chi(a_j - a_k)$$

$$= \sum_{a \in \mathbb{F}_q} \chi(a)\chi(a_j - a_i + a)$$

$$= \begin{cases} -1 & \text{if } i \neq j \\ q - 1 & \text{otherwise} \end{cases}$$

For every $1 \leq i \leq q$ we have

$$\sum_{1 \leq k \leq q} b_{ik} = \sum_{1 \leq k \leq q} \chi(a_i - a_k) = \sum_{c \in \mathbb{F}_q} \chi(c) = 0$$

$$b_{ij} = \chi(a_i - a_j) = \chi(-1)\chi(a_j - a_i) = \chi(-1)b_{ji} = \begin{cases} b_{ji} & \text{if } q \equiv 1 \pmod{4} \\ -b_{ji} & \text{if } q \equiv 3 \pmod{4} \end{cases}.$$
If $q \equiv 1 \pmod{4}$ then the previous equation shows that $B$ is symmetric and we define

$$C = \begin{bmatrix}
0 & 1 & \cdots & 1 \\
1 & \vdots & & B \\
\vdots & & & \vdots \\
1 & & & 1
\end{bmatrix}$$

Now $C$ is symmetric and $CC^\top = qI$ so $C$ is a symmetric conference matrix of order $q + 1$. On the other hand, if $q \equiv 3 \pmod{4}$ then $B$ is antisymmetric and we define

$$C = \begin{bmatrix}
0 & 1 & \cdots & 1 \\
-1 & \vdots & & B \\
\vdots & & & \vdots \\
-1 & & & -1
\end{bmatrix}$$

Now $C$ is antisymmetric and $CC^\top = qI$ so $C$ is an antisymmetric conference matrix of order $q + 1$. It now follows from the previous lemma that the desired Hadamard matrix exists. □