Lecture 14

Hadamard matrices

Definition (H – matrix)

A square $n \times n$ matrix H is called an Hadamard matrix of order n if all the entries of H are ± 1 and $HH^T = nI_n$ where I_n is the identity matrix of order n.

Examples

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

(standard form)

Fact 1 If H is an H-matrix, then H^T is also an H-matrix.

Fact 2 Let A and B be generalized permutation matrices. Then, H is an H-matrix if and only if AHB is an H-matrix.

Definition (H-equivalent)

Two H-matrices H_1 and H_2 are H-equivalent if there exist generalized permutation matrices A and B, s.t.

$H_2 = AH_1B$.

Fact 3 Any H-matrix is H-equivalent to an H-matrix with every entry in the 1st row and 1st column equal to +1.

Proof. Let $I_n(i)$ denote the generalized permutation matrix obtained from I_n by replacing the (i,i) entry with -1. Then, by applying $I_n(i)$ we can change the sign of the i^{th} row and i^{th} column of H, resp. ($I_n(i) \cdot H$ or $H \cdot I_n(i)$.) ∎

Fact 4 (N.C of the existence of an H-matrix)

If H is an H-matrix of order n, then $n = 1$ or 2, or $n \equiv 0 \pmod 4$.

Proof. For $n \geq 4$. W.L.O.G. let H be a standard H-matrix, i.e. all +1's in the 1st row and 1st column. By considering the orthogonality of the first three rows, we conclude the proof. ∎

Conjecture

$\forall\ n \equiv 0 \pmod 4$, there exists an H-matrix of order n.

(Many results have been obtained, but not settled in general.)

Fact 5 (Doubling construction)

If H is an H-matrix of order n, then $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is also an H-matrix which is of order $2n$.

Proof.

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}^T = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} H^T & H^T \\ H^T & (-H)^T \end{pmatrix}$$

$$= \begin{pmatrix} HH^T+HH^T & HH^T-HH^T \\ HH^T-HH^T & HH^T+HH^T \end{pmatrix} = \begin{pmatrix} 2I_n & 0 \\ 0 & 2I_n \end{pmatrix} = 2I_{2n}. \quad \blacksquare$$

Fact 6

For each $n = 2^t$, there exists an H-matrix of order n.

(By Fact 5).

Example

Let $S_\lambda = [s_{i,j}]$ be a matrix. We use $a \otimes S$ to denote the matrix obtained from S, such that $a \otimes S = [a \cdot s_{i,j}]$.

$$S = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \qquad (-1) \otimes S = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

Fact 2 If $M = [m_{i,j}]_{m \times m}$ and $S = [s_{i,j}]_{\lambda \times \lambda}$ are H-matrices, then $M \otimes S$ is also an H-matrix where

$$M \otimes S = \begin{bmatrix} m_{1,1} \otimes S & m_{1,2} \otimes S & \cdots & m_{1,m} \otimes S \\ \vdots & \vdots & & \vdots \\ m_{m,1} \otimes S & m_{m,2} \otimes S & \cdots & m_{m,m} \otimes S \end{bmatrix}$$

. Clearly $M \otimes S$ is of order $m \cdot \lambda$.

Proof. Let $H = (M \otimes S) \cdot (M \otimes S)^T$. Then, $H(i,j)$ (Block form) is equal to

$$\sum_{k=1}^{m} (m_{i,k} \otimes S) \cdot (m_{j,k} \otimes S^T)$$

$$= \sum_{k=1}^{m} m_{i,k} \cdot m_{j,k} \cdot \lambda I_\lambda = \lambda I_\lambda \text{ iff } i = j. \quad \blacksquare$$

Fact 8

There exists an H-matrix of order 12 and therefore there exist H-matrices of order $3 \cdot 2^t$ where $t \geq 2$.

Proof. (Williamson's method)

Let $H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$ where $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ and

$B = C = D = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$.

Now, we have $A^2 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$ and $B^2 = C^2 = D^2 = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$.

Moreover, $AB = BA$, $AC = CA$, $AD = DA$, in fact, all of them are the same, $\begin{bmatrix} -1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & -1 \end{bmatrix}$.

Again, by using the multiplication of block form, we have $H \cdot H^T = \begin{bmatrix} A^2+B^2+C^2+D^2 & & 0 \\ & \ddots & \\ 0 & & A^2+B^2+C^2+D^2 \end{bmatrix} = 12 \cdot I_{12}$.

■

Fact 9

If there exists an H-matrix of order $4k$, then there exists a $2-(4k-1, 2k-1, k-1)$ design.

Proof. Let H be an H-matrix of standard form. Now, by deleting the 1st row and 1st column, and replace all (-1)'s with 0's, we obtain a $(0,1)$-matrix H' of order $4k-1$. (For example, $k=2$, we have

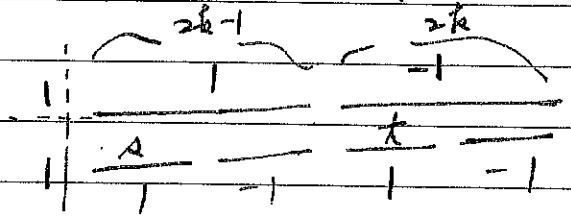
$$H = \left[\begin{array}{c|cccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 \end{array}\right] \rightarrow \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} B_1\ B_2\ B_3\ B_4\ B_5\ B_6\ B_7 \\ \left[\begin{array}{ccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] \end{array} .$$

With the idea of support by assigning row indices as $\mathbb{Z}_{4k-1}$. we have $4k-1$ blocks. So, in the example of $k=2$, the blocks are $\underline{135}, \underline{034}, \underline{236}, \underline{012}, \underline{146}, \underline{056}, \underline{245}$.

As to the design $(X, \mathcal{B})$, we conclude that $|X| = |\mathcal{B}| = 4k-1$, and for each $B \in \mathcal{B}$, $|B| = 2k-1$, since we have $2k-1$ 1's left.

Per-Duet

For the λ of the design $(X, \mathcal{B})$, we observe that in every two rows of H', they have exactly $k-1$ common 1's in order to satisfy the orthogonality in H.



$$1+a=t$$
$$1+a+t=2k$$
$$2+2a=2k$$
$$a=k-1$$

Hence, we have a $2-(4k-1, 2k-1, k-1)$ design, in fact, it is a symmetric design. That is, a symmetric design exists (with certain parameters) if an H-matrix of certain order exists.

(Bonus) Find more H-matrices.