Lecture 13. May 23, 25

Hadamard matrices and Related Designs

Definition (Hadamard matrix)

A square $n \times n$ matrix H is called an Hadamard (or a Hadamard) matrix of order n if all the entries of H are ± 1 and $H \cdot H^T = n \cdot I_n$. (an H-matrix in short.)

Examples:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right]$$

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

Proof. Since $H \cdot H^T = nI$, H is a non-singular matrix. It suffices to show that $H^T \cdot H = n \cdot I_n$. This follows by

$$H^T H = H^{-1}(HH^T)H = H^{-1}(nI_n)H = n \cdot I_n. \quad \blacksquare$$

Fact 2 Let A and B be generalized permutation matrices (square matrices whose entries are $0, 1, -1$ such that in each row and each column there is exactly one nonzero entry). $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ (example)

Then, AHB is an $\mathcal{A}$-matrix provided H is an $\mathcal{A}$-matrix.

Proof. Notice that $AA^T = BB^T = HH^T/n = I_n$. First, it is not difficult to see that all the entries of AHB are either 1 or -1. Next, $(AHB)(AHB)^T = AHBB^TH^TA^T = AHH^TA^T = AnI_n$ $= nI_n$. ∎

Definition ($\mathcal{A}$-equivalent)

Two $\mathcal{A}$-matrices H_1 and H_2 are $\mathcal{A}$-equivalent if there exist generalized permutation matrices A and B such that $H_2 = AH_1B$.

Fact 3 Any $\mathcal{A}$-matrix is $\mathcal{A}$-equivalent to an $\mathcal{A}$-matrix with every entry in the first row and first column equal to $+1$.

Proof. Notice that $I_n(i)$ denote the diagonal matrix in which $I_n(i)_{k,k} = \begin{cases} 0 & \text{if } k \neq k, \\ 1 & \text{if } k = k \neq i, \text{ and} \\ -1 & \text{if } k = k = i. \end{cases}$ Clearly, $I_n(i)$ is a generalized permutation matrix. Furthermore, if H is an $\mathcal{A}$-matrix, then $I_n(i) \cdot H$ is also an $\mathcal{A}$-matrix.

Notice that $I_n(i) \cdot H$ is a matrix obtained from H by replacing the ith row $(h_{i,1}, h_{i,2}, \cdots, h_{i,n})$ of H with $(-h_{i,1}, -h_{i,2}, \cdots, -h_{i,n})$. Similarly, $H \cdot I_n(i)$ is obtained from H by replacing the ith column with negative entries.

Therefore, by applying $I_n(i)$ for suitable $i \in \{1, 2, \cdots, n\}$, we obtain an H-equivalent matrix (to H) in which every entry in the first row and first column equal to "+1". (Standard form!)

Example:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

(The same as the matrix in p.1.)

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

Proof. $n = 1$ $[1]$, $n = 2$, $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Assume that $n > 2$.

By the equivalence relation, we may assume that H is a standard H-matrix, i.e., the first row is $(\underbrace{1, 1, \cdots, 1}_{n})$.

Furthermore, we may let the second row be $(1, 1, \cdots, 1, -1, -1, \cdots, -1)$.

Since the inner product of these vectors is 0, there are equal 1's and (-1)'s. Hence $n = 2m$ for some positive integer m.

Now, consider the 3rd row. (See Figure 1)

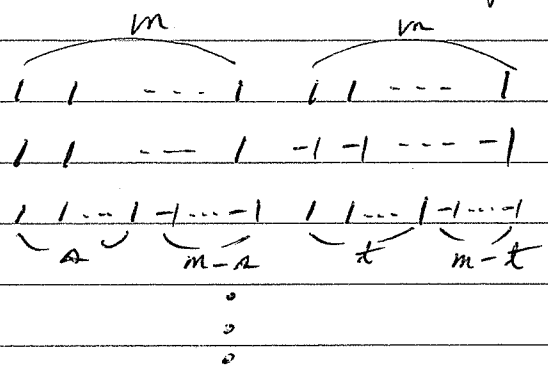

Figure 1

By the assumption of H-matrix, $s + t = (m-s) + (m-t)$, and (1st and 3rd)

$s + m - t = m - s + t$. These two equations imply

$$\begin{cases} 2m = 2(s+t), \\ 2s = 2t. \end{cases}$$

This implies that $m = 2s$ and thus $n \equiv 0 \pmod 4$. ∎

Conjecture on Hadamard matrices

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

Fact 5 If there exists an H-matrix of order m and there exists an H-matrix of order s, then there exists an H-matrix of order $m \cdot s$.

Let $a \otimes S$ denote the matrix obtained from S by multiplying each entry of S with a. For example,

$$(-1) \otimes \underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}}_{H\text{-matrix}} = \underbrace{\begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}}_{H\text{-matrix}}.$$

Let $M = [m_{i,j}]_{m \times m}$. Then $M \otimes S$ is the matrix

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

Hence, $M \otimes S$ is an $ms \times ms$ matrix if S is an $s \times s$ matrix.

Now, we claim that if both M and S are H-matrices, then $M \otimes S$ is also an H-matrix. Consider $H = (M \otimes S) \cdot (M \otimes S)^T$. Then, the (i,j)-entry of H is $\sum_{k=1}^{m} (m_{i,k} \otimes S) \cdot (m_{j,k} \otimes S^T) =$

$$\sum_{k=1}^{m} (m_{i,k} \cdot m_{j,k}) S \cdot S^T = \begin{cases} 0 & \text{if } i \neq j, \text{ and} \\ m \cdot s & \text{if } i = j. \end{cases}$$

∎

Fact 6. If there exists an H-matrix of order n, then there exists an H-matrix of order $2n$.

Fact 7. For each $n = 2^t$, $t \geq 1$, there exists an H-matrix of order n.

How about others?

Exercise 3.1. Find as many H-matrices (of different orders) as possible. (20 points.)

Now, we can use an H-matrix of order n to construct a 2-design of order $n-1$. We start with an example $n = 8$

H:

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	1	−1	−1	−1	−1	1	1
1	−1	−1	1	−1	1	1	−1

$\xrightarrow{H'}$

	1	2	3	4	5	6	7
1	0	1	0	1	0	1	0
2	1	0	0	1	1	0	0
3	0	0	1	1	0	0	1
4	1	1	1	0	0	0	0
5	0	1	0	0	1	0	1
6	1	0	0	0	0	1	1
7	0	0	1	0	1	1	0

H'

Step 1. Delete the 1st row and 1st column.

Step 2. Replace "−1" with "0".

Step 3. Find the supports of each column vector.

2 4 6
1 4 5
3 4 7
1 2 3
2 5 7
1 6 7
3 5 6

So, we obtain a Steiner triple system of order 7.

Fact 8 In general, if we have an H-matrix of order $4(\lambda+1)$, then we have a $2-(4\lambda+3, 2\lambda+1, \lambda)$ design. In fact, this is a symmetric design, i.e. each point occurs in exactly $2\lambda+1$ blocks. ($r=k$, $v=b$)

Proof. Exercise 3.2 (10 points)

Note that $v = 4\lambda+3$ and $k = 2\lambda+1$ are easy to see. (The # of 1's in each column.) It is left to show that any two varieties occur together in exactly λ times.

Since each column of H' corresponds to a block, a pair of elements i and j occur together in blocks is equivalent to count the number of common 1's in row i and row j.

↑ (Hint)

$$b = \frac{\lambda\binom{4\lambda+3}{2}}{\binom{2\lambda+1}{2}} = \frac{\lambda(4\lambda+3)(4\lambda+2)}{(2\lambda+1)(2\lambda)} = 4\lambda+3 = v.$$

Williamson's Method

Consider

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

very important

where A, B, C, D are symmetric matrices.

If for any two matrices X and Y in $\{A, B, C, D\}$, $XY = YX$, then $HH^T = (A^2 + B^2 + C^2 + D^2) \otimes I_4$. Here, if $A = B = C = D = [1]$, then H is an H-matrix of order 4.

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

It is not difficult to check that $AB = BA$, $AC = CA$, $AD = DA$, $BC = CB$, $BD = DB$ and $CD = DC$.

check!

Nothing to check!

$$A^2 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}, \quad B^2 = C^2 = D^2 = \begin{bmatrix} -1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$$

$A^2 + B^2 + C^2 + D^2 = 12 I_3$, Hence, H is an H-matrix of order 12.

$$H^T = \begin{bmatrix} A^T & -B^T & -C^T & -D^T \\ B^T & A^T & D^T & -C^T \\ C^T & -D^T & A^T & B^T \\ D^T & C^T & -B^T & A^T \end{bmatrix}$$

Since A, B, C, D are symmetric, $A^T = A$, $B^T = B$, $C^T = C^T$ and $D^T = D$.

Review the multiplication of matrices can use the "block" form! For example,

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} D & E \\ F & G \end{bmatrix} = \begin{bmatrix} AD+BF & AE+BG \\ CD+DF & CE+DG \end{bmatrix}.$$

Since we can apply the idea of "product", the H-matrices of order $4n$ is difficult when n is odd. So, we consider odd n in what follows.

As mentioned above, if we can find suitable A, B, C, D, then we obtain an H-matrix of order $4 \cdot "n"$ where n is the order of A (resp. B, C, D). That is to say, if we have $n \times n$ matrices A, B, C, D satisfying commute (and symmetric) condition, then we obtain an H-matrix of order $4n$.

The example in previous page is an example when $n = 3$.

How about the other n's?

How to find suitable A, B, C, D?

Let

$$U = \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ 1 & & & & 0 \end{bmatrix}_{n \times n}$$

be a permutation matrix.

Then $U^n = I_n$

For example,

$$\begin{bmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0 \end{bmatrix}\begin{bmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0 \end{bmatrix} = \begin{bmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&0&0&0 \end{bmatrix}$$

$$(12345)\circ(12345) = (13524)$$

Now, let $A = \sum_{i=0}^{n-1} a_i U^i$, $B = \sum_{i=0}^{n-1} b_i U^i$, $C = \sum_{i=0}^{n-1} c_i U^i$, and $D = \sum_{i=0}^{n-1} d_i U^i$. Since $U^T = U^{-1}$, A, B, C, D will be symmetric provided $a_{n-i} = a_i$, $b_{n-i} = b_i$, $c_{n-i} = c_i$ and $d_{n-i} = d_i$.

Check!

So, if all a_i's, b_i's, c_i's and d_i's are ± 1, then we obtain an H-matrix if $A^2 + B^2 + C^2 + C^2 = 4n I_n$.

(Note that we already have an example when $n = 3$.)

Then? We shall stop here. For more details, please refer to Combinatorial Theory (2nd edition) written by M. Jr. Hall.