Hadamard Matrices and Designs

Definition

An n x n matrix H = h_{ij} is an ***Hadamard matrix of order n*** if the entries of H are either +1 or -1 and such that $HH^t = nI$, where H^t is the transpose of H and I is the order n identity matrix.

Put another way, a (+1,-1)-matrix is Hadamard if the inner product of two distinct rows is 0 and the inner product of a row with itself is n.

Examples

A few examples of Hadamard matrices are;

$$\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix} \qquad \begin{matrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{matrix} \qquad \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{matrix}$$

These matrices were first considered as Hadamard determinants. They were so named because the determinant of an Hadamard matrix satisfies equality in Hadamard's determinant theorem, which states that if $X = x_{ij}$ is a matrix of order n where $| x_{ij} | \leq 1$ for all i and j, then

$$| \det X | \leq n^{n/2}.$$

Properties

It is apparent that if the rows and columns of an Hadamard matrix are permuted, the matrix remains Hadamard. It is also true that if any row or column is multiplied by -1, the Hadamard property is retained. [Prove this]

Thus, it is always possible to arrange to have the first row and first column of an Hadamard matrix contain only +1 entries. An Hadamard matrix in this form is said to be ***normalized***.

Order of a Hadamard Matrix

Theorem - The order of an Hadamard matrix is 1,2 or 4n, n an integer.

Proof: [1] is an Hadamard matrix of order 1 and the first example above is an Hadamard matrix of order 2. Suppose now that H is an Hadamard matrix of order h > 2. Normalize H and rearrange the first three rows to look like:

$$\begin{array}{cccc}
1\ .....\ 1 & 1\ .....\ 1 & 1\ .....\ 1 & 1\ .....\ 1 \\
1\ .....\ 1 & 1\ .....\ 1 & -1\ .....{-1} & -1\ .....{-1} \\
1\ .....\ 1 & -1\ .....{-1} & 1\ .....\ 1 & -1\ .....{-1} \\
 & & & \\
x & y & z & w
\end{array}$$

Where x,y,z,w are the numbers of columns of each type.

Order of a Hadamard Matrix

Theorem V.1.1 - The order of an Hadamard matrix is 1,2 or 4n, n an integer.

Proof: (cont) Then since the order is h,

$$x + y + z + w = h$$

and taking the inner products of rows 1 and 2, 1 and 3, and, 2 and 3 we get

$$x + y - z - w = 0$$

$$x - y + z - w = 0$$

$$x - y - z + w = 0.$$

Solving this system of equations gives,

$$x = y = z = w = h/4.$$

Thus, the integer h must be divisible by 4.

Known orders

Corollary. If H is a normalized Hadamard matrix of order 4n, then every row(column) except the first has 2n minus ones and 2n plus ones, further n minus ones in any row (column) overlap with n minus ones in each other row (column).

Proof: This is a direct result of the above proof since any two rows other than the first can take the place of the second and third rows in the proof. The same argument can be applied to the columns.

Hadamard matrices are known for many of the possible orders, the smallest order for which the existence of an Hadamard matrix is in doubt is currently 668 (A solution for the previous unknown case of 428 was announced by Kharaghani and Tayfeh-Rezaie in June 2004).

Kronecker Construction

Construction: Given Hadamard matrices H_1 of order n and H_2 of order m the direct product of these two matrices, represented by:

$$H = H_1 \times H_2 = \begin{matrix} h_{11}H_2 & h_{12}H_2 & \ldots & h_{1n}H_2 \\ h_{21}H_2 & h_{22}H_2 & \ldots & h_{2n}H_2 \\ \ldots & \ldots & \ldots & \ldots \\ h_{n1}H_2 & h_{n2}H_2 & \ldots & h_{nn}H_2 \end{matrix}$$

where $H_1 = | h_{ij}|$, is an Hadamard matrix of order nm.

Proof: [Left as an exercise].

Example

Let

$$H = \begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix} \qquad \text{and} \qquad H^* = \begin{matrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{matrix}$$

then the direct product H x H* is

$$\begin{matrix} H^* & H^* \\ H^* & -H^* \end{matrix}$$

Example

which in full form is,

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

Homework: Starting with the Hadamard matrix of order 2, repeatedly use the direct product construction to construct an Hadamard matrix of order 32.

If an Hadamard has order t then this construction can be used to produce an Hadamard matrix of order 2t.

Quadratic Character of a Field

For odd prime powers q, define the ***quadratic character*** of the field GF(q) as the function χ_q : GF(q) → {-1, 0, 1}

$$\chi_q(x) = \begin{cases} 0 \text{ if } x = 0, \\ 1 \text{ if } x \text{ in } QR(q), \\ -1 \text{ if } x \text{ in } NQR(q). \end{cases}$$

Note:

$\chi_q(-1) = 1$ if $q \equiv 1 \bmod 4$, $\chi_q(-1) = -1$ if $q \equiv 3 \bmod 4$.

The quadratic character is multiplicative,

$$\chi_q(xy) = \chi_q(x)\ \chi_q(y).$$

Quadratic Character of a Field - 2

Further properties of χ_q :

Lemma:

$$1.\ \sum_{x\in GF(q)} \chi_q(x)=0,\ \ \text{and}$$

$$2.\ \sum_{x\in GF(q)} \chi_q(x)\chi_q(x+y)=-1,\ \text{for all}\ y\in GF(q)^*=GF(q)\setminus\{0\}.$$

Pf: Part 1 follows from |QR(q)| = |NQR(q)| = (q-1)/2.
For Part 2, observe
χ_q (x) χ_q (x+y) = χ_q (x) χ_q (x) χ_q (1+yx^{-1}) = χ_q (1+yx^{-1}) if x≠0.
Since y≠0, 1+yx^{-1} takes on all values except 1, so

$$\sum_{x\in GF(q)} \chi_q(x)\chi_q(x+y)=\sum_{x\in GF(q),\,x\neq 0} \chi_q(1+yx^{-1})$$

$$=\sum_{s\in GF(q),\,s\neq 1} \chi_q(s)=\sum_{s\in GF(q)} \chi_q(s)-\chi_q(1)=0-1=-1.$$

Conference Matrix Construction

A ***conference matrix*** of order n is an nxn matrix C with entries in {-1,0,1} such that all diagonal entries are 0 and $CC^T = (n-1)I_n$.

Example:

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{matrix}$$

From the product condition it follows that the only 0's in the matrix will be on the main diagonal.

Conference Matrix Construction -2

Conference matrices are closely related to Hadamard matrices, so it is not surprising that there are similar constraints on the order of conference matrices. In particular we have the following result (without proof):

Theorem: If a symmetric conference matrix of order n exists, then n ≡ 2 mod 4 and n-1 is the sum of two integral squares.

Conference Matrix Construction-3

Construction: For $q \equiv 1 \bmod 4$, define the $q+1$ x $q+1$ matrix $W = w_{ij}$, with indices from GF(q) U $\{\infty\}$, by:

$$w_{ij} = \chi_q(i-j) \text{ for } i,j \,\varepsilon\, GF(q),$$
$$w_{\infty\infty} = 0,\ w_{ij} = 1 \text{ otherwise.}$$

Theorem: If $q \equiv 1 \bmod 4$ is a prime power, then W is a symmetric conference matrix of order q+1.

Pf: Diagonal entries of W are all 0 and every off diagonal element is ±1. Thus, the diagonal entries of WW^T are all q and since -1 is a square, W is a symmetric matrix. So, we must show that the off diagonal entries of WW^T are all 0.

Conference Matrix Construction-4

Theorem: If q ≡ 1 mod 4 is a prime power, then W is a symmetric conference matrix of order q+1.

Pf: (cont) Let i,j in GF(q) i ≠ j, then the (i,j) entry of WW^T is

$$1+\sum_{h\in GF(q)}\chi_q(i-h)\chi_q(j-h)=1+\sum_{x\in GF(q)}\chi_q(x)\chi_q(x+y) \quad \text{where } x=i-h \text{ and } y=j-i$$

$$=1+(-1)=0.$$

For i ≠∞ $w_{i\infty} = w_{\infty i}$ =

$$\sum_{x\in GF(q)}\chi_q(x)=0.$$

Our example was this construction with q = 5.

Conference Matrix Construction -5

Theorem: If C is a symmetric conference matrix of order m then the matrix

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

is an Hadamard matrix of order 2m.

Pf: Since C is symmetric we have $H^T = H$ and every entry of H is ±1. It is straight-forward to check that:

$$HH^t = HH = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Further computation shows that $A = B = (2m)I_m$ giving the required result.

Conference Matrix Construction -6

Combining these results gives us:

Corollary: If m is odd there is an Hadamard matrix of order 4m provided 2m-1 is a prime power.

This gives the following small orders:

m	2m-1	order	m	2m-1	order
3	5	**12**	19	37	**76**
5	9	**20**	21	41	**84**
7	13	**28**	25	49	**100**
9	17	**36**	27	53	**108**
13	25	**52**	31	61	**124**
15	29	**60**			

Williamson's Method

Consider this matrix identity:

$$H = \begin{pmatrix} -a & b & c & d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} \rightarrow HH^{t} = (a^2 + b^2 + c^2 + d^2)\, I_4 .$$

valid for any entries from a commutative ring.

If we can find 4 nxn symmetric commuting matrices with ±1 entries (A, B, C and D) such that $A^2 + B^2 + C^2 + D^2 = 4nI_n$ then an Hadamard matrix of order 4n exists.

Williamson's Method

The Hadamard matrices constructed this way are said to be of Williamson type.

The matrices used in this construction must be circulant matrices (each row is a cyclic permutation of the previous row). While there is an infinite family of Williamson type Hadamard matrices they have not be classified.

Constructions are known for orders: 12, 20, 28, 36, 44, 52, 60, 68, 76, 84, 92, 100, 108, 116, 148, 172, ...

The constructions we have discussed give all orders $\leq$ 100.

Hadamard 2-Designs

Hadamard matrices of order 4t (t > 1) can be used to create symmetric BIBD's, which are called ***Hadamard 2-Designs.***

The construction actually forms the incidence matrix of the BIBD, from which the design is easily obtained. The Hadamard designs have parameters $v = 4t – 1$, $k = 2t - 1$ and $\lambda = t - 1$, or $v = 4t - 1$, $k = 2t$, and $\lambda = t$.

The construction, as we shall see, is reversible, so that BIBD's with these parameters can be used to construct Hadamard matrices.

Construction

Let H be an Hadamard matrix of order 4t. First normalize the matrix H (so that the first row and column are just +1's), then remove the first row and column. The 4t-1 x 4t-1 matrix which remains, say A, has 2t -1's in each row and column and 2t-1 +1's in each row and column, so the row and column sums are always -1 for A. The inner product of two distinct rows of A will be -1 and the product of a row with itself will be 4t-1. These statements are summarized by the matrix equations,

$$AJ = JA^t = -J \quad \text{and} \quad AA^t = 4tI - J$$

where I is the identity matrix and J is the all one matrix of the appropriate order.

Construction

Now construct the matrix B = ½(A + J). B is a (0,1)-matrix, whose row and column sums are 2t-1,
i.e., BJ = JB = (2t-1)J. Furthermore, the matrix equation,

$$BB^t = tI + (t-1)J$$

is satisfied [verify]. Comparing this to an earlier result, we see that B is the incidence matrix of a symmetric (since B is a square matrix) BIBD with v = 4t-1, k = 2t-1 and λ= t-1. Similarly, if C = ½(J - A), C will be the incidence matrix of a (4t-1,2t,t)-design.

Example

Let H be the 8 x 8 Hadamard matrix seen before. In normalized form we have,

$$H = \begin{matrix} + & + & + & + & + & + & + & + \\ + & + & - & - & + & + & - & - \\ + & - & + & - & + & - & + & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & - & + & - & + \\ + & - & - & + & - & + & + & - \end{matrix} \quad A = \begin{matrix} + & - & - & + & + & - & - \\ - & + & - & + & - & + & - \\ - & - & + & + & - & - & + \\ + & + & + & - & - & - & - \\ + & - & - & - & - & + & + \\ - & + & - & - & + & - & + \\ - & - & + & - & + & + & - \end{matrix} \quad B = \begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{matrix}$$

So, labeling the rows of B with {1,2,...,7} we have the (7,3,1)-design whose 7 blocks are:

{1,4,5}   {2,4,6}   {3,4,7}   {1,2,3}   {1,6,7}   {2,5,7}   {3,5,6}

Example

The matrix C is B with the 0's and 1's interchanged (a design obtained by interchanging the 0's and 1's of an incidence matrix is called the complementary design of the original) and its blocks form the (7,4,2)-design:

{2,3,6,7} {1,3,5,7} {1,2,5,6} {4,5,6,7} {2,3,4,5} {1,3,4,6} {1,2,4,7}.

Exercise: Prove that an Hadamard design (i.e. a symmetric BIBD with either of these sets of parameters) can be used to construct an Hadamard matrix.