Hadamard Matrices

Negar Mokhberian , Kosar Kazemi

Sharif University Of Technology , Discrete Mathematics , Professor Foroughmand Araabi

Introduction

In mathematics, a **Hadamard matrix**, named after the French mathematician Jacques Hadamard, is a square matrix with entries from {±1} and have mutually orthogonal row vectors and mutually orthogonal column vectors. In combinatorial terms, it means that every two different rows have matching entries in exactly half of their columns and mismatched entries in the remaining columns. In addition Hadamard was interested in finding the maximal determinant of square matrices with entries from the unit disc, and he showed that this maximal determinant nn/2 was achieved by Hadamard Matrices. Yet they have been actively studied for over 138 years and still have more secrets to be discovered.

The smallest examples are :

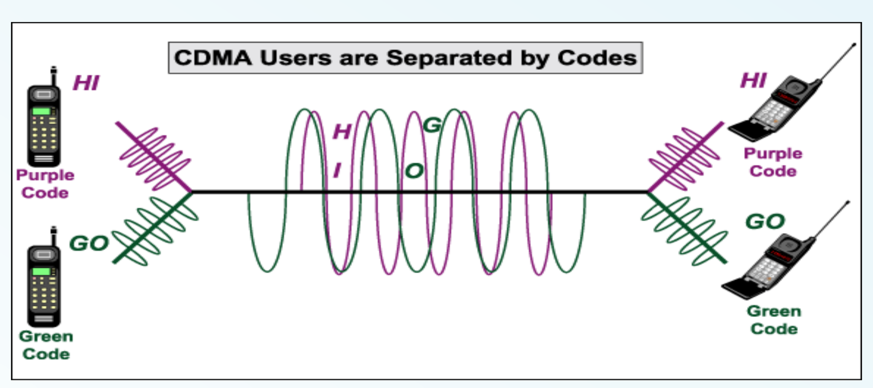
$$\begin{pmatrix} 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix}$$

Let H be a Hadamard matrix of order n. The transpose of H is closely related to its inverse. The correct formula is:

$$H \times H^T = nI_n$$

Code Division Multiple Access (CDMA)

In the last few decades there has been an drastic increase in global use of internet and mobile phone services. One of the biggest challenge faced in communication is to cater to large number of demands at the same time with a limited bandwidth of frequency over which transmission lines and devices can actually operate. Traditional solution this problem like Time Division Multiple Access or Frequency Division Multiple Access are quite slow and unstable. CDMA on the other hand uses the same frequency channel at the same time to send data to many users without any hinderance. In CDMA, data for every user is encoded by multiplying it with a distinct row of a Hadamard matrix. And all the data is sent over the same line. At the destination, users are able to decode the data back by multiplying the encoded message by their row of matrix, because the codes of all the users are orthogonal so, one can only decode it's own message (result of multiplying his row to other messages will be 0) and thus avoid any kind of hinderance.



A necessary condition

Hadamard remarked that such matrices could exist only if n was 1, 2 or a multiple of 4.

Now we prove that the order of a Hadamard matrix H is a member of the set {1, 2, 4k} where k runs through the positive integers.

Proof: [+1] and $\begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$ are Hadamard matrices of orders 1 and 2. For $n > 2$, let the rows of H be $\alpha_1, \alpha_2, \ldots, \alpha_n$. Multiplying any of the columns of H by -1 has no effect on the pairwise orthogonality of the rows, nor does any permutation of the columns of H . For convenience, we multiply those columns of H by -1 where α_1 has a -1, so that in the normalized matrix H' , α'_1= (+1, +1, ... , +1). We also permute the columns so that α'_2 = (+1, +1, ... , +1, -1 , -1 , ... , -1). Since ($\alpha'_1 . \alpha'_2$) = 0 , α'_2 must consist of equally many +l's and -l's, hence n/2 of each, and n must be even. We further permute the columns, without affecting the appearance of α'_1 or α'_2 , to get α'_3 = (+1, ... ,+1,-1, ... ,-1,+1, ... , +1,-1, ... ,-1) where we have r times a "+1" followed by (n/2 - r) times a "-1", and then s times a "+1" followed by (n/2 - s) times a "-1". Since ($\alpha'_1 . \alpha'_3$) = 0, we have ($\alpha'_1 . \alpha'_3$) = (r + s) – (n/2- r) – (n/2- s) = 0 from which r + s =n/2 . Since ($\alpha'_2 . \alpha'_3$) = 0 , we have ($\alpha'_2 . \alpha'_3$) = r – (n/2- r) - s + (n/2- s) = 0 , from which r - s = 0 . Hence r = s =n/4 , and n must be a multiple of 4 .

On Hadamard's conjecture

The most important open question in the theory of Hadamard matrices is that of existence. The Hadamard conjecture proposes that a Hadamard matrix of order n exists if n is 1, 2 or any multiple of 4. All information presently available supports the proposal that the converse of Hadamard's observation is true. Hadamard matrices of orders 12 and 20 were subsequently constructed by Hadamard (in 1893). An example of order 12 is as follows:

$$\begin{pmatrix}
+1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & +1 \\
+1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 \\
+1 & +1 & +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 & +1 & -1 \\
+1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 & +1 & -1 & -1 \\
-1 & +1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & -1 \\
-1 & -1 & +1 & +1 & +1 & +1 & +1 & +1 & -1 & -1 & -1 & +1 \\
+1 & -1 & -1 & +1 & -1 & -1 & +1 & +1 & +1 & -1 & +1 & +1 \\
-1 & +1 & -1 & -1 & +1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 \\
-1 & -1 & +1 & -1 & -1 & +1 & +1 & +1 & +1 & +1 & +1 & -1 \\
+1 & -1 & -1 & -1 & +1 & +1 & +1 & -1 & -1 & +1 & +1 & +1 \\
-1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & +1 & +1 \\
-1 & -1 & +1 & +1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1
\end{pmatrix}$$

In 2005, Hadi Kharaghani and Behruz Tayfeh-Rezaie published their construction of a Hadamard matrix of order 428. As a result, the smallest order for which no Hadamard matrix is presently known is 668.

As of 2008, there are 13 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known. They are: 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, and 1964.

Sylvester's construction

Examples of Hadamard matrices were actually first constructed by James Joseph Sylvester in 1867. Let H be a Hadamard matrix of order n. Then the partitioned matrix

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is a Hadamard matrix of order $2n$. This observation can be applied repeatedly and leads to the following sequence of matrices, also called Walsh matrices.

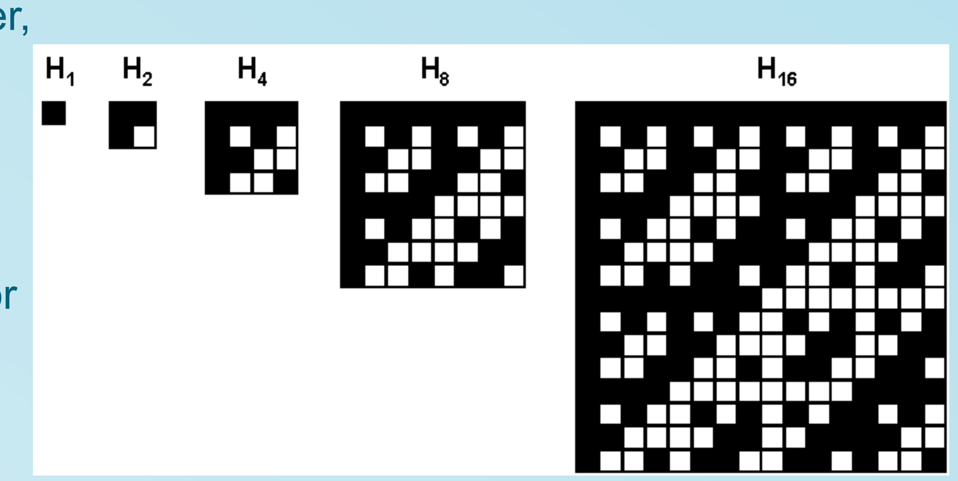
$$H_1 = \begin{pmatrix} 1 \end{pmatrix} \qquad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and

$$H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix} = H_2 \otimes H_{2^{k-1}}$$

For 2≤k , where $\otimes$ denotes the Kronecker product.

In this manner, Sylvester constructed Hadamard matrices of order 2*k* for every non-negative integer *k*.



Using symmetric design

A (square) (v, k, λ)-design is a pair D = (P, B) consisting of a set P = {p1,...,pv} of v points and a set B = {B1,...,Bv} of v blocks each containing k points (1 < k < v), such that each pair of distinct points is contained in exactly λ blocks.

An incidence matrix A = [aij] of D is a v × v matrix with entries 0, 1, having aij =1 if and only if pj ∈Bi.

It follows that a v×v matrix A with entries 0, 1 is an incidence matrix of a (v, k, λ)- design if and only if

$$AA^T = (k-\lambda)I + \lambda J, \quad AJ = kJ$$

where I is the v × v identity matrix and J is the v × v all 1s matrix. This is so much like the equation for Hadamard matrix. In general, this formula allows us to equate the core of a Hadamard matrix of order 4n and the (±1) version of an incidence matrix of a (4n −1, 2n − 1, n − 1)-design. That is, if A′ = 2A − J is the (±1) matrix obtained from incidence matrix A by replacing 0 by −1, then

$$H = \begin{pmatrix} 1 & 1 \\ 1^T & A' \end{pmatrix}$$

is the corresponding Hadamard matrix of order 4n, and vice versa.

Generalized Hadamard matrices

In 2014 an Iranian professor Saieed Akbari and his co-worker Asghar Bahmani published a paper titled "A Generalization of Hadamard Matrices " to generalize Hadamard matrices by introducing S-GHMn .The matrix A is called an S-GHMn if A is a matrix in order m×n and AA^T = Diag(λ1,...,λn), for some positive numbers λi ,i = 1,...,n. In this paper he conjectures that for every positive integer n, there exists a {±1, ±2, ±3}-GHMn. Some of aspects of this generalized hadamards are same as we had in normal one of them (hadamards that all their entries filled by +1 or -1) for example as a theorem in this paper is proved that if C and D are both GHMn such that $CD^T = DC^T$, $CC^T + DD^T$ = Diag (λ1,...,λn), for some positive numbers λi , i = 1,...,n. Then the

matrix A = $\begin{pmatrix} C & D \\ -D & C \end{pmatrix}$ is an S-GHM2n.

This is very similar to Syslvester's construction of Hadamard matrices in order 2^n .

Another theorem in this paper discusses how to obtain generalized Hadamard matrices using symmetric design:

if we Let N be the incidence matrix of a 2−(v, k, λ) symmetric design. Suppose that A is a v × v matrix obtained by replacing 0 and 1 with s and r, respectively in N. Then AA^T = aIv + bJv, where a = (k − λ)(r − s)2 and b=λr2+2(k−λ)rs+(v−2k+λ)s2.

n	S	n	S	n	S	n	S	n	S
1	$\{1\}$	11	$\{?\}$	21	$\{-1,2\}$	31	$\{-3,1,2\}$	41	$\{?\}$
2	$\{\pm1\}$	12	$\{\pm1\}$	22	$\{\pm1,2\}$	32	$\{\pm1\}$	42	$\{\pm1,\pm2\}$
3	$\{-1,2\}$	13	$\{\pm1,\pm2,3\}$	23	$\{-2,1,3\}$	33	$\{?\}$	43	$\{?\}$
4	$\{\pm1\}$	14	$\{\pm1,2\}$	24	$\{\pm1\}$	34	$\{\pm1,\pm2,3\}$	44	$\{\pm1\}$
5	$\{-2,3\}$	15	$\{-1,2\}$	25	$\{?\}$	35	$\{?\}$	45	$\{-1,2\}$
6	$\{-1,2\}$	16	$\{\pm1\}$	26	$\{\pm1,\pm2,\pm3\}$	36	$\{\pm1\}$	46	$\{1,\pm2\}$
7	$\{\pm1,2\}$	17	$\{?\}$	27	$\{?\}$	37	$\{?\}$	47	$\{?\}$
8	$\{\pm1\}$	18	$\{\pm1,\pm2,\pm3\}$	28	$\{\pm1\}$	38	$\{\pm1,2\}$	48	$\{\pm1\}$
9	$\{\pm1,2,3\}$	19	$\{1,\pm2\}$	29	$\{?\}$	39	$\{?\}$	49	$\{?\}$
10	$\{\pm1,2\}$	20	$\{\pm1\}$	30	$\{\pm1,\pm2\}$	40	$\{\pm1\}$	50	$\{?\}$

Constructions of S-GHMn for n ≤ 50

References

- S. Akbari and A.Bahmani ,"A Generalization of Hadamard Matrices ",(2014)
- K.J. Horadam , Hadamard Matrices and Their Applications ,(2006).
- Jennifer Seberry and B.J.Wysocki and T.A.Wysocki , "On some applications of Hadamard matrices " ,(2005) .
- A.Pott , P.V. Kumar , T. Helleseth and D. Jungnickel ,"Difference Sets, Sequences and their Correlation Properties " (1999) .
- *Kenneth H. Rosen, Ph.D.* , " Handbook of Combinatorial Designs ", Second Edition , (2006) .