CONSTRUCTION OF HADAMARD MATRICES

N.V. Ramana Murty[1], V. Gopinath[2], N. R. Sreelatha[3]
[1]Dept. of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh, INDIA
[2]Dept. of Mathematics, Ch.S.D. St. Teressa Autonomous College for Women, Eluru, A.P., INDIA
[3]Technology Analyst, Application Development, INFOSYS, Chennai, T.N., INDIA
E-mail ID: [1]raman93in@gmail.com , [2]gopinath.veeram@gmail.com , [3]nsreelu94@gmail.com

Abstract

Hadamard matrices are a special class of square matrices with entries 1 and -1 only. They have many applications in Coding theory, Physical Sciences, Neuron networks and Computer Science. Therefore, the construction of Hadamard matrices has its own significance. There are many methods to construct these matrices. But, it has been concentrated on Payley's method which is one of the new methods.

Introduction

The name Hadamard matrices came after the name of Jacques Hadamard, a French mathematician. A square matrix of order n with entries 1 and -1 such that $H^T H = HH^T = nI_n$, is called Hadamard matrix, where H^T is the transpose of H and I_n is the identity matrix of order n. Therefore, the scalar product of any two rows or columns is zero. That is, any two rows or columns of a Hadamard matrix are orthogonal.

For example the matrices $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ are Hadamard matrices of order 2 and 4 respectively. It is proved that the value of the determinant of a Hadamard matrix of order n is $n^{n/2}$. Since all the elements of a Hadamard matrix H are 1 and -1, the value of the determinants of H and $-H$ is same. Therefore, if all the elements of first and first column of a Hadamard matrix 1's only, then it is called a normalized Hadamard matrix.

Main Results

Towards the existence of Hadamard matrix we have the following:

Lemma 1: If $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is a Hadamard matrix of order 2, then the matrices

$H_2 = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix}$, $H_3 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix}, \cdots$ are Hadamard matrices of order 2^2, 2^3, and so on.

Proof: Obvious.

For further construction, we need the definition of Legendre symbol.

Definition 2: The Legendre symbol denoted by λ is defined on a finite field F_q containing q elements by

$\lambda(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \text{ is a square}, \\ -1 & \text{if } a \text{ is not a square} \end{cases}$. For example, $\lambda(3) = -1$, $\lambda(4) = 1$, in the field $F_5 = \{0,1,2,3,4\}$ with respect to addition and multiplication modulo 5.

Theorem 3: If $F_q = \{a_0 = 0, a_1, a_2, \cdots, a_{q-1}\}$ is a finite field, containing q elements, with respect to addition and multiplication modulo q, where q is some prime power which is in the form of $4k-1$ for a positive integer k, then the matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & -1 & \lambda(a_1) & \cdots & \lambda(a_{q-2}) & \lambda(a_{q-1}) \\ 1 & \lambda(a_{q-1}) & -1 & \cdots & \lambda(a_{q-3}) & \lambda(a_{q-2}) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \lambda(a_1) & \lambda(a_2) & \cdots & \lambda(a_{q-1}) & -1 \end{bmatrix}$$ of order $(q+1)\times(q+1)$ is a Hadamard matrix.

Proof: Define a matrix M of order q such that the $(i,j)th$ entry of M equals $\lambda(a_i - a_j)$, where λ is the Legendre symbol defined on the field F_q. Now, construct the matrix $S = -[M + I_q]$, where I_q is the unit matrix of q, and hence S of order $q \times q$. Then, we see that the matrix $H = \begin{bmatrix} 1 & 1 \\ 1 & S \end{bmatrix}$ is the required Hadamard matrix.

Example 4: If $k = 3$, then $q = 4k - 1 = 11^1 = 11$. Therefore, consider the finite field $F_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$ with respect to addition and multiplication modulo 11. Then we get the Hadamard matrix of order 12.

Therefore, the matrix $M =$

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

Therefore the matrix, $S = \begin{bmatrix} -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \end{bmatrix}$

Hence, the matrix $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \end{bmatrix}$ of order 12.

Note: From the above example we see that all Hadamard matrices need not be symmetric.

Definition 3: If $A = \left[a_{ij} \right]$ and B be any two matrices, then the direct product of the matrices A, B is denoted by $A \otimes B$ and it is defined as $A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \cdots & \cdots & \cdots \end{bmatrix}$.

Method 2

Theorem 4: If p^m is a prime power and $p^m - 1$ is divisible by 4, then there exists a Hadamard matrix of order $2\left(p^m + 1 \right)$.

Proof: Define a matrix M of order p^m such that the $(i, j)th$ entry of M equals $\lambda\left(a_i - a_j \right)$, where λ is the Legendre symbol defined on the field F_{p^m}. Now, construct the matrix $S = \begin{bmatrix} 0 & 1 \\ 1 & M \end{bmatrix}$, of order $p^m + 1$.

and hence S of order p^m. Then, we see that the matrix $H = S \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + I_{p^m+1} \otimes \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$ is the required Hadamard matrix of order $2\left(p^m+1\right)$.

Example 5: If $p=5, m=1$ then $p^m - 1 = 5^1 - 1 = 4$ which is divisible by 4. Therefore, we get a Hadamard matrix of order $2\left(5^1+1\right)=12$. Since $p^m = 5$, we consider the finite field $F_5 = \{0,1,2,3,4\}$ with respect to addition and multiplication modulo 5, containing 5 elements. Since $\lambda(1)=1=\lambda(4)$, $\lambda(2)=-1=\lambda(3)$, the matrix M is given by $M = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{bmatrix}$. Now $S = \begin{bmatrix} 0 & 1 \\ 1 & M \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}$.

Therefore, by Theorem 4 $H = \begin{bmatrix} 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \end{bmatrix}$ of order 12.

References

[1] Sloane, N. J. A., M. Harwit, Masks for Hadamard transform optics, and weighing designs, Applied Optics, 15 (1976),, 107 -114

[2] Van Lint, J.H., Introduction to Coding theory (Second Edition) (1992), Springer-Verlag, New York

[3] Folk,R., A. Karatashov, P.Linsonek and P.Paule, Symmetries in Neural Networks: A Linear Group Action Approach, J.Phys.A.Math.Gen.26(1993),3159-3164

[4] Rudolf Lidl, Gunter Pilz, Appliied Abstract Algebra (Second Edition) (1998), Springer-Verlag, New York

[5] Charles Lanski, Concepts in Abstract Algebra, Cengage Learning, Inc., Florence, KY, U.S(2004)

[6] P.M. Cohn, Further Algebra and Applications, Springer, 2004

[7] David S.Dummit, Richard M.Foote, Abstract Algebra, John Wiley and sons, NewYork, 2005