Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

Subseries: USSR
Adviser: L.D. Faddeev, Leningrad

1168

S.S. Agaian

Hadamard Matrices and Their Applications

Springer-Verlag
Berlin Heidelberg New York Tokyo

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

Subseries: USSR
Adviser: L.D. Faddeev, Leningrad

1168

S.S. Agaian

Hadamard Matrices and Their Applications

Springer-Verlag
Berlin Heidelberg New York Tokyo

Author

S.S. Agaian
Computer Center of the Academy of Sciences
Sevak str. 1, Erevan 44, USSR

Consulting Editor

D.Yu. Grigorev
Leningrad Branch of the Steklov Mathematical Institute
Fontanka 27, 191011 Leningrad, D-11, USSR

Mathematics Subject Classification (1980): 05XX; 05BXX

ISBN 3-540-16056-6 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-16056-6 Springer-Verlag New York Heidelberg Berlin Tokyo

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2146/3140-543210

CONTENTS

Introduction

The importance of orthogonal matrices in modern discrete mathematics and its applications is well known; for many applied problems (for example, for construction of discrete equipments realizing fast or orthogonal transformations) one needs consideration of integer orthogonal matrices and in particular, orthogonal matrices with the elements -1 and +1. Square orthogonal matrices with the elements -1 and +1 are called Hadamard matrices.

Investigations of Hadamard matrices were connected initially with a linear algebra problems (for example, with finding maximum of determinant). Later on it turned out that the applications of Hadamard matrices in questions connected with information transfer by non-line electromagnetic waves, with automaton training and with a number of question from information theory (information compression and noiseless coding, optimal linear detection of a signal through noise, construction of multiple-access chanels) are also fruitful. Besides it turned out that there are interrelations between Hadamard matrices and different combinatorial configurations such as block-designs, Latin squares, orthogonal F-square configurations, correcting codes, finite geometties, strongly regular graphs. These interrelations allow to investigate the properties of different objects using the analogy in their structures.

Recently a considerable increase of investigation devoted to Hadamard matrices has occured. Some problems connected with (classic, generalized, high-dimensional) Hadamard matrices are still unanswered; so, till now it is not known if there exist Hadamard matrices of order n for all n divisible by 4.

Historically, first work devoted to Hadamard matrices was due to Sylvester who in 1867 proposed a recurrent method for construction of Hadamard matrices of order 2^k. In XIX century the following papers

also appeared: the work of Scarpis (1898) proving that if $p=3 \pmod 4$ or $p=1 \pmod 4$ is a prime number then there is an Hadamard matrix of order $p+1$ and $p+3$, respectively; the work of Hadamard (1893) where the following result in particular is stated: if $A=\{a_{i,j}\}_{i,j=1}^{n}$, $|a_{i,j}| \leq M$, $a_{i,j}$ are real numbers for any i, j, then the absolute value of determinant A is less or equal to $M^n n^{n/2}$. Hadamard has proved that this bound is within the reach only for Hadamard matrices. This result gives rise to the term "Hadamard matrix".

In 1933 Paley stated that the order of any Hadamard matrix is divisible by 4. There are some reasons to assume that the reverse statement is also true. This problem is called Hadamard problem (sometimes Sylvester or Paley problem) and is till now unanswered although there are over 1500 papers devoted to it. Introduction to the topic under discussion are books Hall (1970), Ryser (1963); it should be noted that these surveys have not included the works of Soviet authors and also a series of interesting applications stimulating interest in this problem.

A principal difficulty of this problem and many other combinatorial problems is the lack of unified methods for construction of Hadamard matrices of order $4n$ for all n. The known methods of construction are applicable only to relatively "rare" sequences on n. For many n it is usually necessary to develop a direct method of construction sometimes using the machine access. There are only a few papers where recurrent methods of construction for Hadamard matrices are introduced. These methods use the following branches of mathematics: number theory, group theory, combinatorial analysis. There exist practically no papers devoted to combination of direct and recurrent methods. The list of known Hadamard matrices of order n, $n \leq 4000$, constructed by a computer was given in Wallis (1978), where he noted that the minimal order for which the existence of an Hadamard matrix is not known is 268.

The known methods of Hadamard matrix construction can be divided into Williamson, Baumert-Hall-Goethals-Seidel, Paley-Wallis-Whiteman methods and Golay-Turyn, Plotkin and J.Wallis approaches.

This work provides a survey of papers devoted to (classic, generalized, high-dimensional) Hadamard matrices and discusses some new results in the topic. Specifically, attention is paid to the questions of construction of Hadamard matrices with prescribed properties. Besides, the method of construction must be simple and has to allow an effective realization in the sence of rate and memory of the computer.

The work presented consists of 3 chapters and 9 sections. In § 2 we will consider a new approach to construction of Hadamard matrices uniting two above-mentioned methods namely, Williamson and Baumert-Whiteman method. In § 3 we will generalize and strengthen Golay-Turyn, Wallis and Plotkin methods. In particular, we will solve in this section the reverse problem: from the codes we will construct Hadamard matrices, prove a theorem allowing for an arbitrary g_i, $i=1,2$ to find a lower limit for existence of type $2^s q_1^{k_1}$, $2^s q_1^{k_1} \cdot q_2^{k_2}$ (k_i are arbitrary natural numbers) Hadamard matrices of all orders, propose a recurrent method for construction of δ-codes and T-matrices of new orders. In § 4 new block (sufficiently simple in construction) method is proposed combined the direct and recurrent methods of Hadamard matrices construction. The method allows to state firstly that there exists a Hadamard matrix of order 12 for which there doesn't exist a partition D(12,4) generating this matrix (that is, the refusation of second Plotkin hypothesis) and secondly, that from the existence of two Hadamard matrices of order m_1, m_2 follows the existence of an Hadamard matrix of order $m_1 \cdot m_2/2$.

In §§ 2 - 4 we will give also recurrent formulae of construction of Williamson matrices, Baumert-Hall, Goethals-Seidel, Wallis, Wallis-Whiteman arrays of new orders allowing to construct infinite classes of Hadamard matrices. The block method posseses a definite universa-

lity allowing to construct different orthogonal systems providing fast algorithms for calculation of partial Fourier sums by these systems.

§ 5 is devoted to investigation of generalized Hadamard matrices and Butson problem. In particular, some necessary conditions of the existence for generalized Hadamard matrices H(p,h) (p is not a prime number) are given, recurrent methods of construction of circulant, block-circulant generalized Hadamard matrices of new orders are obtained.

In § 6 the block method is extended to a high-dimensional case which allows to construct new classes of high-dimensional regular and irregular Hadamard matrices. A solution of Schlichta problem is given, the upper and lower bounds of weight density and excess density of (classic and high-dimensional) Hadamard matrices are obtained.

In §§ 7 - 9 we will introduce some applications (information compressing. noiseless coding, optimal linear detection of the signals through noise, construction of multiple- access channels and so on) of Hadamard matrices where the leading part is played by fast algorithms for calculations of Hadamard transformations.

Finally, some unanswered problems are formulated.

The author would like to express his sincere gratitude to S.V. Yablonskiy on whose initiative this work was prepared and to V.M.Sidelnikov, V.A.Zinovjev, who have read the manuscript and made a series of valuable notes.

§ 1. Basic definitions, notations and auxiliary results

NOTATIONS. I - is a unit matrix; J - is a square matrix containing only ones (in case of need the dimension of matrix is indicated by a subscript);

$$R = \begin{Vmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{Vmatrix}, \qquad U = \begin{Vmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 1 \end{Vmatrix} \tag{1}$$

It can be shown that we have

PROPERTY 1. For every k, k=1,2,...n-1, n is an odd number, there exists a unique s such that $(U^s)^2 = U^k$,

PROPERTY 2. There exists a matrix P such that PUP*=D where

$$D = \begin{Vmatrix} \gamma_1 & 0 & \dots & 0 & 0 \\ 0 & \gamma_2 & \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & \dots & \gamma_{n-1} & 0 \\ 0 & 0 & \dots & 0 & \gamma_n \end{Vmatrix}$$

and $\gamma_1, \gamma_2, \dots, \gamma_n$ are different n-th roots of unity. $e_n=(1,1,\dots,1)$ is a row-vector of length n; T is a transposition sign; x is a Kronecker product [120]; $\otimes$ is a matrix product defined as

$$A \otimes X = \begin{Vmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,m} \\ A_{2,1} & A_{2,2} & \dots & A_{2,m} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{m,2} & A_{m,2} & \dots & A_{m,m} \end{Vmatrix} \otimes \begin{Vmatrix} X_1 \\ X_2 \\ \cdot \\ \cdot \\ X_m \end{Vmatrix} = \sum_{i=1}^{m} \begin{Vmatrix} A_{1,i} * X_i \\ A_{2,i} * X_i \\ \cdot \\ \cdot \\ A_{m,i} * X_i \end{Vmatrix} \tag{2}$$

* is an Hadamard product [311], that is if $A=(a_{i,j})_{i,j=1}^{n}$, $B=(b_{i,j})_{i,j=1}^{n}$ then

$$A * B = (a_{i,j} \cdot b_{i,j})_{i,j=1}^{n} \tag{3}$$

Let A, B, C, D be square (-1, +1) matrices. Let

$$W[4] = \begin{Vmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{Vmatrix} \tag{4}$$

denotes a Williamson array [318],

$$GZ[4] = \begin{Vmatrix} A & BR & CR & DR \\ -BR & A & -D^{T}R & C^{T}R \\ -CR & D^{T}R & A & -B^{T}R \\ -DR & -C^{T}R & B^{T}R & A \end{Vmatrix} \tag{5}$$

denotes Goethals-Seidel array of order 4 [113],

$$BY[4] = \begin{Vmatrix} A & B & C & D \\ -B^{T} & A^{T} & -D & C \\ -C & D^{T} & A & -B^{T} \\ -D^{T} & -C & B^{T} & A^{T} \end{Vmatrix} \tag{6}$$

denotes a Wallis-Whiteman array of order 4 [311], and

$$WA[4] = \begin{Vmatrix} A_1 \times B_1 & A_2R \times B_2 & A_3R \times B_3 & A_4R \times B_4 \\ -A_2R \times B_2 & A_1 \times B_1 & A_4^{T}R \times B_4 & -A_3^{T}R \times B_3 \\ -A_3R \times B_3 & -A_4^{T}R \times B_4 & A_1 \times B_1 & A_2^{T}R \times B_2 \\ -A_4R \times B_4 & A_3^{T}R \times B_3 & -A_2^{T}R \times B_2 & A_1 \times B_1 \end{Vmatrix} \tag{7}$$

denotes a Wallis array of order 4 [299].

A Radon function is defined by equation $\rho(m)=8c+2^{d}$, where $m=2^{a}b$, $a=4c+d$, $d\leq 3$ and b is an odd number. Note that $\rho(m)=m$, if $m=1,2,4,8$, $\rho(16)=9$ and $\rho(2^{a}b)=\rho(2^{a})$, if b is an odd number.

DEFINITION 1. An Hadamard matrix of order m is a mxm matrix H_m with elements -1 and +1 such that

$$H_m H_m^T = H_m^T H_m = mI_m \tag{8}$$

Expression (8) is equal to the statement that every two rows and hence, every two columns of matrix H_m are orthogonal. Obviously, permutation of rows or columns of H_m and multiplication by -1 preserves this property.

Following geometrical interpretation may be given for the expression (8). If we assume that row elements of matrix H_m represent vector coordinates of Euclidean m-space with orthonormal base, then determinent $\det H_m$ is (up to sign) the volume of m-parallelepiped constructed on these vectors. The property (8) shows that the volume of the parallelepiped is product of lengths its edges originating from the common vertex. An Hadamard matrix is said to be of skew-symmetric type, if

$$H_m = I_m + S_m, \qquad S_m^T = -S_m \tag{9}$$

DEFINITION 2. A rectangular mxn matrix $H_{m,n}$ consisting of -1 and +1 is said to be a rectangular (or incomplete) Hadamard matrix, if

$$H_{m,n} H_{m,n}^T = nI_m$$

DEFINITION 3 [120] Matrices H_1 and H_2 are said to be equivalent Hadamard matrices, if $H_2 = PH_1Q$, where P and Q are monomial permutation matrices with elements -1 and +1. Such a Hadamard matrix is said to be normalized.

The concept of equivalence leads to the question of finding for a given order n the number of non-equivalent Hadamard matrices of order n. So, in 1961 Hall has proved that there are 5 classes of equivalence for Hadamard matrices of order 16 and in 1965 he has shown the existence of 3 classes for matrices of order 20. The basic results in this question one can find in following papers: Rutledge (1952), Stiffler and Baumert (1961), Baumert (1962), Wallis and Wallis (1969), Bussemaker and Deidel (1970), Newman (1971), Wallis (1971a), (1971b), (1972a),

(1972b).

Other concepts and applications of equivalence (integral equivalence, weight equivalence) one can find in following papers: Gordon (1971), Norman (1976), Longyear (1978), Cooper, Milas and Wallis (1978), Yang (1977) and Y.Wallis (1977).

Let (V,B) be a pair of sets $V=\{a_1,a_2,\ldots,a_v\}$, $B=\{B_i\}_{i=1}^{c}$

$B_i \subset V$. element a_i and block B_j are incident, if $a_i \in B_j$.

DEFINITION 4. (V,B) is said to be a balanced incomplete block design or a B I B-design with parameters V,B,Z,K,S if

1. each block B_j contains identical number of K-elements,

2. each element a_i belongs to the same number r of blocks,

3. for each non-ordered pair a_i, a_j of various elements the number of blocks containing this pair is S.

A block design is called symmetric, if V=B,K=r.

A set of integers $D=\{x_1,x_2,\ldots x_k\}$ is called a difference set with parameters (v,k,s), if for every $d\in\{1,2,\ldots n-1\}$ there are precisely s pair of $x_i,x_j \in D^2$ such that $x_i-x_j \equiv d(\mathrm{mod}n)$.

The information about block designs and difference sets one can find in [61, 120, 311].

DEFINITION 5.[125]. An orthogonal design of order m of type $(s_1, s_2,\ldots s_n)$, $s_i>0$, i=1,2,...n is a square matrix A_m of order m with commutative in pairs elements from set $\{0,\pm x_1, \pm x_2,\ldots \pm x_n\}$ provided

$$A_m A_m^T = \sum_{i=1}^{n} s_i x_i^2 I_m$$

The information about the orthogonal designs one can find in [124-131].

DEFINITION 6.[4]. Square (0,-1,+1) matrices G_i, i=1,2,...l of order m satisfying following conditions:

1. $G_i * G_j = 0$, $i \neq j$, $i,j = 1,2,\ldots,l$

2. $G_i G_j^T - G_j G_i^T = 0$, $i,j=1,2,\ldots,l$

3. $\sum_{i=1}^{l} G_i$ is (-1,+1) matrix of order m.

4. $\sum_{i=1}^{l} G_i G_i^T = mI_m$

Will be called a l-elemental hyperframe of order m.

The l-elemental hyperframe $\{G_i\}_{i=1}^{l}$ of order m has following properties:

1. $\{H \times G_i\}_{i=1}^{l}$ is a l-elemental hyperframe of order km, where H is an Hadamard matrix of order k.

2. m=0(mod 2).

DEFINITION 7. Matrices S_1 and S_2 of order 2n×n consisting of elements (0,-1,+1) will be called S-matrices, provided

1. $S_1 * S_2 = 0$

2. S_1+S_2 is a (-1,+1) matrix

3. $S_1S_1^T + S_2S_2^T = nI_{2n}$

Let us note only 2 properties of S-matrices.

1. The order of S-matrix satisfies the condition n≡0(mod 2).

2. If there exists an Hadamard matrix of order m, then there exists a S-matrix of order $m \times \frac{m}{2}$.

DEFINITION 8.[295]. Square (-1,+1) matrices $A_i \times B_i$, i=1,2,3,4 of order mn are F-matrices provided

1. A_i, i=1,2,3,4 are circulant (-1,+1) matrices of order m.

2. $B_iB_j^T = B_jB_i^T$, i,j= 1,2,3,4

3. $\sum_{i=1}^{4} (A_i \times B_i)\ (A_i \times B_i)^T = 4mnI_{mn}$

DEFINITION 9 [120].Square (0,-1,+1) matrices X_1, X_2, X_3, X_4 of order k are T-matrices provided

1. $X_i * X_j = 0$, $i \neq j$, i,j=1,2,3,4

2. $\sum_{i=1}^{4} X_i$ is a (-1,+1) matrix of order k.

3. $X_iX_j=X_jX_i$, i,j=1,2,3,4

4. $\sum_{i=1}^{4} X_iX_j^T = kI_k$

DEFINITION 10. [114]. (-1,+1) Sequences $\{a_k\}_{k=1}^{m}$ and $\{b_k\}_{k=1}^{m}$ are supplementary Golay sequences of length m provided

$$\sum_{i=1}^{m-j} (a_i a_{i+j} + b_i b_{i+j}) = 0, \quad j=1,2,\ldots,m-1$$

§ 2. Methods of construction for Hadamard matrices

In this paragraph you can find the review of basic methods of construction of classic Hadamard matrices (see definition 1). Namely, of Williamson method and its modifications, of Baumert-Hall-Goethals-Seidel and Paley-Wallis-Whiteman methods. A new concept of construction of Hadamard matrices is proposed. It combines the Williamson method and that of Baumert-Hall-Goethals-Seidel and presents an unified method allowing also to strengthen the Paley-Wallis-Whiteman method. This concept gives in particular a recurrent way of construction the Williamson matrices, the Baumert-Hall, Goethals-Seidel, Wallis-Whiteman arrays of new orders from which in turn one can produce the infinite classes of Hadamard matrices of new orders, for example of order $4n \prod_i (n_i^{m_i})$, n, n_i are orders of constructed Williamson matrices, $m_i > 0$.

2.1. Williamson method and its modifications

This method is based on a theorem has been proved by Williamson in 1944.

THEOREM 2.1 [120].Let square (-1,+1) matrices W_i, i=1,2,3,4, of order m are

1. circulant, that is $W_i = \sum_{j=0}^{m-1} V_j^{(i)} U^j$, i=1,2,3,4 (2.0)

2. symmetric, that is $V_{m-j}^{(i)} = V_j^{(i)}$, j=1,2,...,m-1, i=1,2,3,4 (2.1)

and meet

3. $\sum_{i=1}^{4} W_i^2 = 4mI_m$ (2.2)

Then a Williamson array $W[W_1, W_2, W_3, W_4]$ is an Hadamard matrix of order 4m.

This theorem shows that the problem of construction of Hadamard mat-

rices of order 4m can be reduced to the construction of square (-1,+1) matrices W_i, i=1,2,3,4 of order m with conditions (2.0), (2.1), (2.2).

Now consider the construction of matrices W_i, i=1,2,3,4 satisfying the conditions of Theorem 2.1.

We denote

$$V_i = PW_iP^*, \quad i= 1,2,3,4 \tag{2.4}$$

where P is an unitary matrix satisfying the property 2. We have from (2.1)

$$V_i = \sum_{j=1}^{m-1} V_j^{(i)} D^j , \quad i= 1,2,3,4 \tag{2.5}$$

From (2.5) the matrices V_i, i= 1,2,3,4 are in particular diagonal and

$$\sum_{i=1}^{4} V_i^2 = 4mI_m , \tag{2.6}$$

that is

$$\sum_{i=1}^{4} \sum_{j=0}^{m-1} V_j^{(i)} \gamma_k^j \Big)^2 = 4m \tag{2.7}$$

Note that relation (2.7) is true for every γ_k hence, for γ_k=1 namely,

$$\sum_{i=1}^{4} \Big(\sum_{j=0}^{m-1} V_j^{(i)} \Big)^2 = 4m \tag{2.8}$$

is true.

Now we have from relation $V_j^{(i)} \in \{-1,+1\}$every bracket is a square of the difference between the positive (p_i) and negative (n_i) terms of the sum, that is

$$\sum_{i=1}^{4} (p_i-n_i)^2 = 4m \tag{2.9}$$

On the other hand Lagrange theorem [120]shows that every positive number is representable as the sum of 4 squares of integers; moreover if m is odd, then 4m is representable as the 4 squares of odd numbers,

that is

$$4m = q_1^2 + q_2^2 + q_3^2 + q_4^2 \tag{2.10}$$

So, we have from (2.8), (2.9) and (2.10)

$$\sum_{j=0}^{m-1} V_j^{(i)} = \sum_{i=1}^{4} (P_i - n_i) = \pm q_i \tag{2.11}$$

Further, from symmetry of W_i matrices we have

$$\begin{aligned}
V_o^{(1)} + 2 \sum_{j=1}^{(m-1)/2} V_j^{(1)} &= \pm q_1 \\
V_o^{(2)} + 2 \sum_{j=1}^{(m-1)/2} V_j^{(2)} &= \pm q_2 \\
V_o^{(3)} + 2 \sum_{j=1}^{(m-1)/2} V_j^{(3)} &= \pm q_3 \\
V_o^{(4)} + 2 \sum_{j=1}^{(m-1)/2} V_j^{(4)} &= \pm q_4
\end{aligned} \tag{2.12}$$

Now we discuss the choice of sign for q_i, i=1,2,3,4, it is easy to verify that

a) for $m \equiv 3 \pmod 4$, $s=(m-1)/2$

$$V_o^{(i)} + 2 \sum_{j=1}^{s} V_j^{(i)} = \begin{cases} q_i, & \text{if } [q_i - V_o^{(i)}]/2 \text{ is odd} \\ -q_i, & \text{if } [q_i + V_o^{(i)}]/2 \text{ is odd} \end{cases} \tag{2.13}$$

b) for $m \equiv 1 \pmod 4$, $s=(m-1)/2$

$$V_o^{(i)} + 2 \sum_{j=1}^{s} V_j^{(i)} = \begin{cases} -q_i, & \text{if } [q_i + V_o^{(i)}]/2 \text{ is even,} \\ q_i, & \text{if } [q_i - V_o^{(i)}]/2 \text{ is even} \end{cases} \tag{2.14}$$

Note that expressions $[q_i \pm V_o^{(i)}]/2$, i=1,2,3,4 for both $m \equiv 3 \pmod 4$ and $m \equiv 1 \pmod 4$ can not be even and odd respectively, and number of positive and negative elements consisting the collection $(V_1^{(i)}, V_2^{(i)}, \ldots, V_{s-1}^{(i)}, V_s^{(i)})$ are $l_i^{(1)}$, $L_i^{(2)}$ respectively, where