Theory and Applications of Higher -Dimensional Hadamard Matrices

Yixian Yang

SCIENCE PRESS
Beijing

Yixian Yang

Theory and Applications of Higher-Dimensional Hadamard Matrices

SCIENCE PRESS
Beijing

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, China
Second Printed in 2006

Printed in Beijing

ISBN 7-03-006782-7 (Science Press, Beijing)

Preface

Just over one hundred years ago, in 1893, Jacques Hadamard found 'binary' (±1) matrices of orders 12 and 20 whose rows (resp. columns) were pairwise orthogonal. These matrices satisfy the determinantal upper bound for 'binary' matrices. Hadamard actually proposed the question of seeking the maximal determinant of matrices with entries on the unit circle, but his name has become associated with the question concerning real (binary) matrices. Hadamard was not the first person to study these matrices. For example, J. J. Sylvester had found, in 1857, such row (column) pairwise orthogonal binary matrices of all orders of powers of two. Nevertheless, Hadamard proved that binary matrices with a maximal determinant could exist only for orders 1, 2, and $4t$, t a positive integer.

With regard to the practical applications of Hadamard matrices, it was M. Hall, Jr., L. Baumert, and S. Golomb who sparked the interest in Hadamard matrices over the past 30 years. They made use of the Hadamard matrix of order 32 to design an eight bit error-correcting code for two reasons. First, error-correcting codes based on Hadamard matrices have good error correction capability and good decoding algorithms. Second, because Hadamard matrices are (±1)-valued, all the computer processing can be accomplished using additions and subtractions rather than multiplication.

Walsh matrices are the simplest and most popular special kinds of Hadamard matrices. Walsh matrices are generated by sampling the Walsh functions, which are families of orthogonal complete functions. Based on the Walsh matrices, a very efficient orthogonal transform, called Walsh–Hadamard transform, was developed. The Walsh–Hadamard transform is now playing a more and more important role in signal processing and image coding.

P. J. Shlichta discovered in 1971 that there exist higher-dimensional binary arrays which possess a range of orthogonality properties. In particular, P. J. Shlichta constructed 3-dimensional arrays with the property that any sub-array obtained by fixing one index is a 2-dimensional Hadamard matrix. The study of higher-dimensional Hadamard matrices was mainly motivated by another important paper of P. J. Shlichta 'Higher-Dimensional Hadamard Matrices', which was published in *IEEE Trans. on Inform.*, in 1979. Since then a lot of papers on the existence, construction, and enumeration of higher-dimensional Hadamard matrices have been reported. For example, J.Hammer and J. Seberry, found, in 1982, that higher-dimensional orthogonal designs can be used to construct higher-dimensional Hadamard matrices. To the author's knowledge much of the research achievements on higher-dimensional Hadamard matrices have been accomplished by S. S. Agaian, W. De Launey, J. Hammer, J. Seberry, Yi Xian Yang, K.J. Horadam, P. J. Shlichta, J. Jedwab, C. Lin, Y. Q. Chen, and others. Many new papers have been published, thus none can collect together all of the newest results in this area.

The book divides naturally into three parts according to the dimensions of Hadamard matrices processed.

The first part, Chapter 1 and Chapter 2, lay stress upon the classical 2-dimensional cases. Because quite a few books (or chapters in them) have been published which introduce the progress of (2-dimensional) Hadamard matrices, we prefer to present an introductory survey rather than to restate many known long proofs. Chapter 1 introduces Walsh matrices and Walsh transforms, which have been widely used in engineering fields. Fast algorithms for Walsh transforms and various useful properties of Walsh matrices are also stated. Chapter 2 is about (2-dimensional) Hadamard matrices, especially their construction, existence, and their generalized forms. The updated strongest Hadamard construction theorems presented in this chapter are helpful for readers to understand how difficult it is to prove or disprove the famous Hadamard conjecture.

The second part, Chapters 3 and 4, deals with the lower-dimensional cases, e.g., 3-, 4-, and 6-dimensional Walsh and Hadmard matrices and transforms. One of the aims of this part is to make it easier to smoothly move from 2-dimensional cases to the general higher-dimensional cases. Chapter 3 concentrates on the 3-dimensional Hadamard and Walsh matrices. Constructions based upon direct multiplication, and upon recursive methods, perfect binary arrays are introduced. Another important topic of this chapter is the existence and construction of 3-dimensional Hadamard matrices of orders $4k$ and $4k + 2$, respectively. Chapter 4 introduces a group of transforms based on 2-, 3-, 4-, and 6-dimensional Walsh–Hadamard matrices and their corresponding fast algorithms. The algebraic theory of higher-dimensional Walsh–Hadamard matrices is presented also.

Finally, the third part, which is the key part of the book, consists of the last two chapters (Chapter 5 and 6). To the author's knowledge, the contents in this part (and the previous second part) have never been included in any published books. This part is divided into chapters according to the orders of the matrices (arrays) processed. Chapter 5 investigates the N-dimensional Hadamard matrices of order 2, which have been proved equivalent to the well known H–Boolean functions and the perfect binary arrays of order 2. This equivalence motivates a group of perfect results about the enumeration of higher-dimensional Hadamard matrices of order 2. Applications of these matrices to feed forward networking, stream cipher, Bent functions and error correcting codes are presented in turn. Chapter 6, which is the longest chapter of the book, aims at introducing Hadamard matrices of general dimension and order. After introducing the definitions of the regular, proper, improper, and generalized higher-dimensional Hadamard matrices, many theorems about the existence and constructions are presented. Perfect binary arrays, generalized perfect arrays, and the orthogonal designs are also used to construct new higher-dimensional Hadamard matrices. The last chapter of the book is a concluding chapter of questions, which includes a list of open problems in the study of the theory of higher-dimensional Hadamard matrices. We hope that these research problems will motivate further developments.

In order to satisfy readers with this special interest, we list, at the end of each chapter, as many up to date references as possible.

I would like to thank my supervisors, Professors. Zhen Ming Hu and Jiong Pang Zhou for their guidance during my academic years at the Information Security Center of Beijing University of Posts and Telecommunications (BUPT). During my research years in higher-dimensional Hadamard matrices I benefited from Professors W. De Launey, J. Hammer, J. Seberry, K. J. Horadam, P. J. Shlichta, J. Jedwab. My thanks go to many of their papers, theses and communications. I was attracted into the area of higher-dimensional Hadamard matrices by P.J. Shlichta's paper 'Higher-Dimensional Hadamard Matrices' published in *IEEE Trans. on Inform. Theory.* My first journal paper was motivated by J. Hammer and J. Seberry's paper 'Higher-Dimensional Orthogonal Designs and Applications' published in *IEEE Trans. on Inform. Theory.* It is Dr. J. Jedwab's wonderful Ph.D thesis 'Perfect Arrays, Barker Arrays and Difference Sets' that motivated me to finish the first book on higher-dimensional Hadamard matrices. One of my main aims in this book is to motivate other authors to begin to publish more books on higher-dimensional Hadamard matrices and their applications, so that the readers in other areas can know what has been done in the area of higher-dimensional Hadamard matrices.

I specially thank my wife, Xin Xin Niu, and my son, Mu Long Yang, for their support. It is not hard to imagine how much they have sacrificed in family life during the past years. I would like to dedicate this book to my wife and son. Finally, I also dedicate this book to my parents, Mr. Zhong Quan Yang and Mrs. De Lian Wei for their love.

Contents

Preface ix

Part I Two-Dimensional Cases 1

Chapter 1 Walsh Matrices 2

1.1 Walsh Functions and Matrices 2

1.1.1 Definitions 3

1.1.2 Ordering 9

1.2 Orthogonality and Completeness 14

1.2.1 Orthogonality 14

1.2.2 Completeness 15

1.3 Walsh Transforms and Fast Algorithms 17

1.3.1 Walsh Ordered Walsh–Hadamard Transforms 18

1.3.2 Hadamard Ordered Walsh–Hadamard Transforms . 20

Bibliography 20

Chapter 2 Hadamard Matrices 22

2.1 Definitions 23

2.1.1 Hadamard Matrices 23

2.1.2 Hadamard Designs 28

2.1.3 Williamson Matrices 34

2.2 Construction 43

2.2.1 General Constructions 43

2.2.2 Amicable Hadamard Matrices 47

2.2.3 Skew Hadamard Matrices 51

2.2.4 Symmetric Hadamard Matrices 53

2.3 Existence 56

2.3.1 Orthogonal Designs and Hadamard Matrices 56

2.3.2 Existence Results 63

Bibliography 66

Part II Lower-Dimensional Cases 71

Chapter 3 Three-Dimensional Hadamard Matrices 72

3.1 Definitions and Constructions 72

3.1.1 Definitions 72

3.1.2 Constructions Based on Direct Multiplications 75

3.1.3 Constructions Based on 2-Dimensional Hadamard Matrices 80

3.2 Three-Dimensional Hadamard Matrices of Order $4k + 2$ .. 83

3.3 Three-Dimensional Hadamard Matrices of Order $4k$ 86

3.3.1 Recursive Constructions of Perfect Binary Arrays .. 86

3.3.2 Quasi-Perfect Binary Arrays 92

3.3.3 3-Dimensional Hadamard Matrices Based on PBA($2^m, 2^m$) and PBA($3.2^m, 3.2^m$) 98

3.4 Three-Dimensional Walsh Matrices 103

3.4.1 Generalized 2-Dimensional Walsh Matrices 103

3.4.2 3-Dimensional Walsh Matrices 108

3.4.3 3-Dimensional Pan–Walsh Matrices 115

3.4.4 Analytic Representations 118

Bibliography 125

Chapter 4 Multi-Dimensional Walsh–Hadamard Transforms 127

4.1 Conventional 2-Dimensional Walsh–Hadamard Transforms 127

4.1.1 2-Dimensional Walsh–Hadamard Transforms 127

4.1.2 Definitions of 4-Dimensional Hadamard Matrices . 130

4.2 Algebraical Theory of Higher-Dimensional Matrices 132

4.3 Multi-Dimensional Walsh–Hadamard Transforms 147

4.3.1 Transforms Based on 3-Dimensional Hadamard Matrices 148

4.3.2 Transforms Based on 4-Dimensional Hadamard Matrices 149

4.3.3 Transforms Based on 6-Dimensional Hadamard Matrices 153

Bibliography 157

Part III General Higher-Dimensional Cases 158

Chapter 5 n-Dimensional Hadamard Matrices of Order 2 ... 159
5.1 Constructions of 2^n Hadamard Matrices 159
5.1.1 Equivalence Between 2^n Hadamard Matrices and H–Boolean Functions 160
5.1.2 Existence of H–Boolean Functions 162
5.1.3 Constructions of H–Boolean Functions 174
5.2 Enumeration of 2^n Hadamard Matrices 180
5.2.1 Classification of 2^4 Hadamard Matrices 180
5.2.2 Enumeration of 2^5 Hadamard Matrices 191
5.2.3 Enumeration of General 2^n Hadamard Matrices .. 192
5.3 Applications 198
5.3.1 Strict Avalanche Criterion and H–Boolean Functions 199
5.3.2 Bent Functions and H–Boolean Functions 205
5.3.3 Reed-Muller Codes and H–Boolean Functions 211
Bibliography 217

Chapter 6 General Higher-Dimensional Hadamard Matrices 219
6.1 Definitions, Existences and Constructions 220
6.1.1 n-Dimensional Hadamard Matrices of Order $2k$ ... 220
6.1.2 Proper and Improper n-Dimensional Hadamard Matrices 238
6.1.3 Generalized Higher-Dimensional Hadamard Matrices 244
6.2 Higher-Dimensional Hadamard Matrices Based on Perfect Binary Arrays 248
6.2.1 n-Dimensional Hadamard Matrices Based on PBAs 248
6.2.2 Construction and Existence of Higher-Dimensional PBAs 251
6.2.3 Generalized Perfect Arrays 264
6.3 Higher-Dimensional Hadamard Matrices Based on Orthogonal Designs 293
6.3.1 Definitions of Orthogonality 294
6.3.2 Higher-Dimensional Orthogonal Designs 299
6.3.3 Higher-Dimensional Hadamard Matrices from Orthogonal Designs 304
Bibliography 313

Concluding Questions 315
Index 317

Part I
Two-Dimensional Cases

Chapter 1
Walsh Matrices

Walsh matrices are the simplest and most popular special kind of Hadamard matrices, which is defined as the (± 1)-valued orthogonal matrix. Walsh matrices are generated by sampling the Walsh functions, which are families of orthogonal complete functions. The orders of Walsh matrices are always equal to 2^n, where n is a non-negative integer. If the $+1$s in a Walsh matrix are replaced by -1s and -1s by 1s, then a good error correcting code with Hamming distance $m/2$, where m is the order of the matrix, is constructed. Walsh matrices are widely used in communications, signal processing, and physics, and have an extensive and widely scattered literature. This chapter concentrates on the definitions, generations and ordering of Walsh matrices, and on Walsh transforms with fast algorithms.

1.1 Walsh Functions and Matrices

Walsh functions belong to the class of piecewise constant basis functions which were developed in the nineteen twenties and have played an important role in scientific and engineering applications. The foundations of the field of Walsh functions were made by Rademacher (in 1922), Walsh (in 1923), Fine (in 1945), Paley (in 1952), and Kaczmarz and Steinhaus (in 1951). The engineering approach to the study and utilization of these functions was originated by Harmuth (in 1969), who introduced the concept of sequence to represent the associated, generalized frequency defined as one half the mean rate of zero crossings. Possible applications of Walsh functions to signal multiplexing, bandwidth compression, digital filtering, pattern recognition, statistical analysis, function approximation, and others are suggested and extensively examined.

1.1.1 Definitions

In order to define the Walsh functions we introduce, at first, a family of important orthogonal (but incomplete) functions which are called Rademacher functions ([1]):

$$\mathrm{RAD}(n,t) = \mathrm{sign}[\sin(2^n\pi t)], n = 0,1,\ldots, \tag{1.1}$$

where sign$[x]$ is the sign function of x, i.e., sign$[x] = 1$ if $x > 0$ and sign$[x] = -1$ if $x < 0$.

Clearly, Rademacher functions are derived from sinusoidal functions which have identical zero crossing positions. Rademacher functions have two arguments n and t such that $R(n,t)$ has 2^{n-1} periods of square wave over a normalized time base $0 \le t \le 1$. The amplitudes of the functions are $+1$ and -1. The first function $R(0,t)$ is equal to one for the entire interval $0 \le t \le 1$. The next and subsequent functions are square waves having odd symmetry.

Rademacher functions are periodic with period 1, i.e.,

$$\mathrm{RAD}(n,t) = \mathrm{RAD}(n,t+1).$$

They are also periodic over shorter intervals such that

$$\mathrm{RAD}(n,t+m2^{1-n}) = \mathrm{RAD}(n,t), \quad n = 1,2,\ldots; \quad m = \pm 1, \pm 2, \ldots$$

Rademacher functions can also be generated using the recurrence relation

$$\mathrm{RAD}(n,t) = \mathrm{RAD}(1,2^{n-1}t)$$

with

$$\mathrm{RAD}(1,t) = \begin{cases} 1, t \in [0,1/2) \\ -1, t \in [1/2,1). \end{cases}$$

In order to define the Walsh functions we note that each integer n, $0 \le n \le 2^m - 1$, has a unique binary extension of the form

$$n = \sum_{k=0}^{m-1} n_k 2^k, \quad \text{where} \quad n_k = 0 \text{ or } 1. \tag{1.2}$$

Then the n-th Paley-ordered Walsh function is defined by

$$\mathrm{Wal}_{\mathrm{P}}(n,t) = \prod_{k=0}^{m-1} [\mathrm{RAD}(k+1,t)]^{n_k}. \tag{1.3}$$

For example, because $7 = 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$,

$$\begin{aligned}\mathrm{Wal}_{\mathrm{P}}(7,t) &= \mathrm{RAD}(3,t)\mathrm{RAD}(2,t)\mathrm{RAD}(1,t)\\ &= \mathrm{sign}[\sin(2^3\pi t)] \times \mathrm{sign}[\sin(2^2\pi t)] \times \mathrm{sign}[\sin(2^1\pi t)].\end{aligned}$$

Thus Walsh functions form an ordered set of rectangular waveforms taking only two amplitude values +1 and −1. Unlike the Rademacher functions the Walsh rectangular waveforms do not have unit mark–space ratio. Like the sine and cosine functions, two arguments are required for complete definition, a time period, t, and an ordering number, n, related to frequency in a way which is described later.

The Walsh functions can also be defined by their time argument. In fact, each non-negative real number t, $0 \leq t < 1$, can be uniquely decomposed as

$$t = \sum_{k=1}^{\infty} t_k 2^{-k}, \quad \text{with} \quad t_k = 0 \text{ or } 1. \tag{1.4}$$

Then the Rademacher functions are derived by

$$\begin{cases}\mathrm{RAD}(0,t) = 1\\ \mathrm{RAD}(k,t) = (-1)^{t_k}, k = 1, 2, \ldots .\end{cases} \tag{1.5}$$

Hence by setting Equation (1.5) into Equation (1.3), we have the following equivalent definition of the Paley-ordered Walsh functions ([1]):

$$\mathrm{Wal}_{\mathrm{P}}(n,t) = (-1)^{\sum_{k=0}^{m-1} n_k t_{k+1}}. \tag{1.6}$$

A straightforward consequence of Equation (1.6) is the following identity:

Lemma 1.1.1 ([2] , [3], [4]) *Let q and n be two non-negative integers. Thus*

$$\mathrm{Wal}_{\mathrm{P}}(n,t)\mathrm{Wal}_{\mathrm{P}}(q,t) = \mathrm{Wal}_{\mathrm{P}}(q \oplus n, t) \tag{1.7}$$

where $q \oplus n$ is the dyadic summation of q and n, i.e., $q \oplus n = k$ if and only if their binary extensions $q = (q_0, q_1, \cdots, q_{m-1})$, $n = (n_0, n_1, \ldots, n_{m-1})$, and $k = (k_0, k_1, \ldots, k_{m-1})$ satisfy $(n_i + q_i)\mathrm{mod}2 = k_i$ for all $0 \leq i \leq m-1$.

Thus the set of Paley-ordered Walsh functions forms an Abelian group under the multiplication operation.

Let k, $0 \leq k \leq 2^m - 1$, be an integer with its binary extension being $k = \sum_{i=0}^{m-1} k_i 2^i$. Then, by Equation (1.6), the discrete sampling of a Walsh function $\mathrm{Wal}_\mathrm{P}(n,t)$ at the point $t = k/2^m$ is

$$W_\mathrm{P}(n,k) = (-1)^{\sum_{i=0}^{m-1} n_i k_{m-1-i}}. \tag{1.8}$$

Therefore by sampling the continuous Walsh functions with the unit space $1/2^m$ we have the following (± 1)-valued matrix of size $2^m \times 2^m$:

$$W_\mathrm{P} = [W_\mathrm{P}(n,k)] = [(-1)^{\sum_{i=0}^{m-1} n_i k_{m-1-i}}]. \tag{1.9}$$

This matrix is called the Paley ordered Walsh matrix.

For example, if $m = 3$, then the corresponding Paley ordered Walsh matrix is

$$W_\mathrm{P} = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & + & - & + & - \\ + & - & + & - & - & + & - & + \\ + & - & - & + & + & - & - & + \\ + & - & - & + & - & + & + & - \end{bmatrix}.$$

Theorem 1.1.1 ([2] , [3], [4]) *Let $W_\mathrm{P} = [W_\mathrm{P}(n,k)]$, $0 \leq n,k \leq 2^m - 1$, be a Paley-ordered Walsh matrix. Then*

1. $W_\mathrm{P}(n,k) = W_\mathrm{P}(k,n)$ *for all* $0 \leq n,k \leq 2^m - 1$, *i.e. the Paley ordered Walsh matrix is symmetrical;*

2. $W_\mathrm{P}(n,k)W_\mathrm{P}(n,q) = W_\mathrm{P}(n,k \oplus q)$ *for all* $0 \leq n,k,q \leq 2^m - 1$, *i.e. the set of columns of the Paley-ordered Walsh matrix is also closed under the bit-wise multiplication;*

3. *The matrix W_P is (± 1)-valued and orthogonal. In other words, W_P is an Hadamard matrix.*

Proof. The first two statements are direct consequences of Equation (1.9). The third statement is owed to the second statement and the following identity:

$$\begin{aligned}\sum_{k=0}^{2^m-1} W_p(n,k) &= \sum_{k=0}^{2^m-1} (-1)^{\sum_{i=0}^{m-1} n_i k_{m-1-i}} \\ &= \sum_{k_0=0}^{1} \cdots \sum_{k_{m-1}=0}^{1} (-1)^{\sum_{i=0}^{m-1} n_i k_{m-1-i}} \\ &= \prod_{i=0}^{m-1} \sum_{k_i=0}^{1} (-1)^{n_i k_{m-1-i}} \\ &= 0 \text{ (provided that } n_i \neq 0 \text{ for some } i).\end{aligned}$$

In other words, except for the all ones row (the 0-th row), the rows of the matrix W_p are balanced by 1 and -1. **Q.E.D.**

The set of Walsh function series produced by Equation (1.5) or equivalently by Equation (1.3) can also be obtained in several other different ways, each of which has its own particular advantages. The methods considered in the following context are:

1. By means of a difference equation;

2. Through the Hadamard matrices;

Both of these derivations are, of course, mathematical processes for which computational algorithms can be developed and the series produced using the digital computer or obtained directly by using digital logic.

From Difference Equations: ([2], [3], [4], [5]) This method gives the function directly in sequence order. Sequence is a term used for describing a periodic repetition rate which is independent of waveform. It is defined as, 'One half of the average number of zero crossings per unit time interval'. From this we see that frequency can be regarded as a special measure of sequency applicable to sinusoidal waveforms only. Applying the definition of sequency to periodic and a periodic function, we obtain:

1. The sequency of a periodic function equals one half the number of sign changes per period;

2. The sequency of an a periodic function equals one half the number of sign changes per unit time, if this limit exists.