数学与现代科学技术丛书 3

Theory and Applications of Higher-Dimensional Hadamard Matrices

(Second Edition)

（高维哈达玛矩阵理论与应用）

Yixian Yang Xinxin Niu and Chengqing Xu

科学出版社
www.sciencep.com

数学与现代科学技术丛书 3

Yixian Yang, Xinxin Niu and Chengqing Xu

Theory and Applications of Higher-Dimensional Hadamard Matrices

(Second Edition)

(高维哈达玛矩阵理论与应用)

SCIENCE PRESS
Beijing

《数学与现代科学技术丛书》已出版书目

1．量子纠错码　冯克勤　陈　豪　著　2010年3月

2．生物计算——生物序列的分析方法与应用　杨　晶　胡　刚　王　奎　沈世镒　编著　2010年3月

3．Theory and Applications of Higher-Dimensional Hadamard Matrices (高维哈达玛矩阵理论与应用)　Yixian Yang, Xinxin Niu and Chengqing Xu　2010年4月

《数学与现代科学技术丛书》序

当代数学在向纵深发展的同时，被空前广泛地应用于几乎一切领域. 一方面，它与其他学科交汇，形成了许许多多交叉学科(例如，信息科学、计算机科学、系统科学、数学物理、数学化学、生物数学、数学语言学、数量经济学、金融数学、复杂性科学、科学计算等)；另一方面，它又被应用于高新技术的开发(例如，信息安全、信息传输、图像处理、语音识别、网络、海量数据处理、网页搜索、遥测遥感、交通管理、医疗诊断、手术方案、药物检验、商业广告等方面)，成为一些高新技术的核心. 应用数学的这种发展趋势急剧地扩展了数学的疆界，也深刻地改变了数学的面貌.

中国的经济正在迅猛发展，其中的科技含量也与日俱增. 为了提高自主创新能力，我国已经有不少数学工作者投身于这类应用数学的研究中，还有更多的数学工作者则正在密切关注这方面的进展，看好它的前景. 愈来愈多的人希望了解这类应用数学的现状，寻找入门之径.

《数学与现代科学技术丛书》是力图反映这个发展趋势的一套应用数学丛书，它将较全面地向我国读者介绍当今数学在现代科学技术各个领域中应用的状况，通过必要的准备知识，逐步把读者引向相关的研究前沿.

从事交叉学科研究和高新技术开发的应用数学家，除了要精通所需的数学知识外，还必须深入了解其所研究问题的来龙去脉. “建模”是应用数学研究实际问题的关键. 这也是一门数学艺术：从复杂的实际问题中抽象出关键的“量的关系”，使得既能反映出问题的基本特征，又能用现阶段的数学工具加以处理. 有鉴于此，这套丛书的一个特点就是：不但要介绍有关的数学理论和方法，还必须介绍问题的来源与背景、数学建模以及如何运用数学工具来解决实际问题.

本丛书适用于数学及相关专业的大学生和研究生，以及与数学有关的各专业科技工作者.

张恭庆

2009 年 11 月

Preface to the Second Edition

Time is flying! Eight years have passed since the publication of the first edition of my book, *Theory and Applications of Higher-Dimensional Hadamard Matrices.*

During the past eight years, my group and I have been applying the Hadamard related theory to many engineering projects and lucky to get quite a few good results, especially in the design and analysis of perfect digital signals and arrays for communications, radars, cryptology, and information security. Thus when the editor of Science Press invited me to republish the book, my colleague and I were very happy to revise the book.

Compared with the first edition, a new part (Part IV) with two new chapters (Chapter 7 and Chapter 8) has been added. In this new version, we concentrate on higher dimensional Hadamard matrices and their applications in telecommunications and information security. This revised book is naturally divided into four parts according to the dimensions of Hadamard matrices processed and applications.

The first part concentrates on the classical 2-dimensional Walsh and Hadamard matrices. Fast algorithms, updated constructions, existence results and their generalized forms are presented for Walsh and Hadamard matrices. Some useful dyadic operation tools are presented, e.g., dyadic additions and dyadic groups. New Hadamard designs based on dyadic addition sets and difference family are also stated here.

The second part 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. This part concentrates on the 3-dimensional Hadamard and Walsh matrices. Constructions based upon direct multiplication, and upon recursive methods, and perfect binary arrays are also introduced. Another important topic of this part is the existence and construction of 3-dimensional Hadamard matrices of orders $4k$ and $4k+2$, respectively, and a group of transforms based on 2-, 3-, 4-, and 6-dimensional Walsh-Hadamard matrices and their corresponding fast algorithms. Different new sequences and arrays are introduced, e.g., the optical orthogonal codes, periodic complementary binary array family, dyadic complementary sequence family, and Bent complementary functions.

The third part is the key part, which 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. After introducing the definitions of the regular, proper, improper, and generalized higher-dimensional Hadamard matrices, many theorems about their 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 other content of this part is the Boolean approach of Hadamard matrices, including the correlation immunity of Boolean functions and Boolean substitutions, stream and block ciphers based on Hadamard matrices, the applications of Hadamard matrices in error-correcting codes, and image coding.

The fourth part states some examples of applications of Hadamard-related ideas to the designs and analysis of 1-dimensional sequences (Chapter 7) and 2-dimensional arrays (Chapter 8). Specifically, enumerations, constructions and correlation immunities of Boolean functions, corresponding to the n-dimensional matrix of order 2, with cryptographic significance are presented in Section 7.1. The correlation functions of Bent-like sequences (including the Gold-Geometric sequences, Generalized Geometric sequences, and p-ary d-form sequences) are calculated in Section 7.2. Hadamard-like difference sets are used in Section 7.3 to construct sequences pairs with mismatched filtering which are, in fact, semi-arrays with two-level autocorrelation functions and good cross-correlations. A few unusual sequences analyses are listed in Section 7.4–especially the implementations of Boolean functions by neural networks, the calculations of linear complexities of sequences represented by the truth tables of Boolean functions, the estimations of upper and lower bounds of periodic ambiguity functions of EQC-Based TFHC, and the properties of auto-, cross- and triple-correlations of sequences. Constructions, correlations, and enumerations of Costas arrays are established in Section 8.1. Section 8.2 concentrates on the parameters, bounds and constructions of optical orthogonal codes, which are families of arrays with good auto- and cross-correlations. Besides the applications stated in Part 4, the theory and ideas of Hadamard matrices can be used in many other areas of communications and information security.

Many open problems in the study of the theory of higher-dimensional Hadamard matrices are also listed in the book. We hope that these research problems will motivate further developments.

The authors would like to give their thanks to the following research foundations, by which this book has been supported: (1) National Basic Research

Program of China (973 Program) (No. 2007CB310704, 2007CB311203); (2) National Natural Science Foundation of China (No. 60673098, 90718001, 60821001, 60731160626); (3) Specialized Research Fund for the Doctoral Program of Higher Education (No. 20070013005, 20070013007); (4) The 111 Project (No. B08004); (5) The National 863 (No. 2007AA01Z430).

Yixian Yang

Preface to the First Edition

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, 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 Hall, Baumert, and 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 the 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.

Shlichta discovered in 1971 that there exist higher-dimensional binary arrays which possess a range of orthogonality properties. In particular, 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 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, Hammer and 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 Agaian, De Launey, Hammer, Seberry, Yixian Yang, Horadam, Shlichta, Jedwab, Lin, 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, concentrates 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, and 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 their 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 Zhenming Hu and Jiongpang 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 De Launey, Hammer, Seberry, Horadam, Shlichta, Jedwab. My thanks go to many of their papers, theses and communications. I was attracted into the area of higher-dimensional Hadamard matrices by Shlichta's paper, "Higher-Dimensional Hadamard Matrices" published in *IEEE Trans. on Inform. Theory.* My first journal paper was motivated by Hammer and Seberry's paper "Higher-Dimensional Orthogonal Designs and Applications" published in *IEEE Trans. on Inform. Theory.* It is Dr. 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, Xinxin Niu, and my son, Mulong 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. Zhongquan Yang and Mrs. De Lian Wei, for their love.

Yixian Yang

Contents

Part I 2-Dimensional Cases

Part II Lower-Dimensional Cases

Part IV Applications to Signal Design and Analysis

Part I

2-Dimensional Cases

Chapter 1

Walsh Matrices

Walsh matrices are the simplest and the most popular special kind of Hadamard matrices, which are 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 laid 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 sequency 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]:

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