

Hadamard Transforms

Hadamard Transforms

Sos Aghaian

Hakob Sarukhanyan

Karen Egiazarian

Jaakko Astola

SPIE
PRESS

Bellingham, Washington USA

To our families for their love, affection, encouragement, and understanding.

Library of Congress Cataloging-in-Publication Data

Hadamard transforms / Sos Aгаian ... [et al.].
p. cm. – (Press monograph ; 207)
Includes bibliographical references and index.
ISBN 978-0-8194-8647-9
1. Hadamard matrices. I. Aгаian, S. S.
QA166.4.H33 2011
512.9'434–dc22

2011002632

Published by

SPIE
P.O. Box 10
Bellingham, Washington 98227-0010 USA
Phone: +1 360.676.3290
Fax: +1 360.647.1445
Email: Books@spie.org
Web: <http://spie.org>

Copyright © 2011 Society of Photo-Optical Instrumentation Engineers (SPIE)

All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means without written permission of the publisher.

The content of this book reflects the work and thoughts of the author(s). Every effort has been made to publish reliable and accurate information herein, but the publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon. For the latest updates about this title, please visit the book's page on our website.

Printed in the United States of America.

First printing



Contents

Preface	xi
Acknowledgments	xiii
Chapter 1 Classical Hadamard Matrices and Arrays	1
1.1 Sylvester or Walsh–Hadamard Matrices	1
1.2 Walsh–Paley Matrices	11
1.3 Walsh and Related Systems.....	13
1.3.1 Walsh system.....	15
1.3.2 Cal–Sal orthogonal system.....	17
1.3.3 The Haar system	24
1.3.4 The modified Haar “Hadamard ordering”.....	29
1.3.5 Normalized Haar transforms.....	30
1.3.6 Generalized Haar transforms	32
1.3.7 Complex Haar transform.....	32
1.3.8 k^n -point Haar transforms.....	32
1.4 Hadamard Matrices and Related Problems	34
1.5 Complex Hadamard Matrices	38
1.5.1 Complex Sylvester–Hadamard transform	39
1.5.2 Complex WHT	41
1.5.3 Complex Paley–Hadamard transform.....	42
1.5.4 Complex Walsh transform	42
References	45
Chapter 2 Fast Classical Discrete Orthogonal Transforms	51
2.1 Matrix-Based Fast DOT Algorithms	52
2.2 Fast Walsh–Hadamard Transform	54
2.3 Fast Walsh–Paley Transform.....	62
2.4 Cal–Sal Fast Transform.....	70
2.5 Fast Complex HTs	75
2.6 Fast Haar Transform.....	79
References	86
Chapter 3 Discrete Orthogonal Transforms and Hadamard Matrices	93
3.1 Fast DOTs via the WHT	94

3.2	FFT Implementation	95
3.3	Fast Hartley Transform	106
3.4	Fast Cosine Transform	115
3.5	Fast Haar Transform.....	122
3.6	Integer Slant Transforms	129
3.6.1	Slant HTs.....	130
3.6.2	Parametric slant HT	131
3.7	Construction of Sequential Integer Slant HTs.....	136
3.7.1	Fast algorithms	141
3.7.2	Examples of slant-transform matrices	142
3.7.3	Iterative parametric slant Haar transform construction.....	143
	References	147
Chapter 4 “Plug-In Template” Method: Williamson–Hadamard Matrices		155
4.1	Williamson–Hadamard Matrices	156
4.2	Construction of 8-Williamson Matrices	168
4.3	Williamson Matrices from Regular Sequences.....	173
	References	182
Chapter 5 Fast Williamson–Hadamard Transforms		189
5.1	Construction of Hadamard Matrices Using Williamson Matrices...	189
5.2	Parametric Williamson Matrices and Block Representation of Williamson–Hadamard Matrices	192
5.3	Fast Block Williamson–Hadamard Transform.....	195
5.4	Multiplicative-Theorem-Based Williamson–Hadamard Matrices...	199
5.5	Multiplicative-Theorem-Based Fast Williamson–Hadamard Transforms.....	202
5.6	Complexity and Comparison.....	206
5.6.1	Complexity of block-cyclic, block-symmetric Williamson–Hadamard transform	206
5.6.2	Complexity of the HT from the multiplicative theorem.....	208
	References	209
Chapter 6 Skew Williamson–Hadamard Transforms		213
6.1	Skew Hadamard Matrices	213
6.1.1	Properties of the skew-symmetric matrices	213
6.2	Skew-Symmetric Williamson Matrices	215
6.3	Block Representation of Skew-Symmetric Williamson–Hadamard Matrices	217
6.4	Fast Block-Cyclic, Skew-Symmetric Williamson–Hadamard Transform.....	219
6.5	Block-Cyclic, Skew-Symmetric Fast Williamson–Hadamard Transform in Add/Shift Architectures	222
	References	224

Chapter 7	Decomposition of Hadamard Matrices	229
7.1	Decomposition of Hadamard Matrices by $(+1, -1)$ Vectors	230
7.2	Decomposition of Hadamard Matrices and Their Classification	237
7.3	Multiplicative Theorems of Orthogonal Arrays and Hadamard Matrix Construction	243
	References	247
Chapter 8	Fast Hadamard Transforms for Arbitrary Orders	249
8.1	Hadamard Matrix Construction Algorithms	249
8.2	Hadamard Matrix Vector Representation	251
8.3	FHT of Order $n \equiv 0 \pmod{4}$	256
8.4	FHT via Four-Vector Representation	263
8.5	FHT of Order $N \equiv 0 \pmod{4}$ on Shift/Add Architectures	266
8.6	Complexities of Developed Algorithms	268
	8.6.1 Complexity of the general algorithm	268
	8.6.2 Complexity of the general algorithm with shifts	270
	References	270
Chapter 9	Orthogonal Arrays	275
9.1	ODs	275
	9.1.1 ODs in the complex domain	278
9.2	Baumert–Hall Arrays	280
9.3	A Matrices	282
9.4	Goethals–Seidel Arrays	289
9.5	Plotkin Arrays	293
9.6	Welch Arrays	295
	References	301
Chapter 10	Higher-Dimensional Hadamard Matrices	309
10.1	3D Hadamard Matrices	311
10.2	3D Williamson–Hadamard Matrices	312
10.3	3D Hadamard Matrices of Order $4n + 2$	318
10.4	Fast 3D WHTs	325
10.5	Operations with Higher-Dimensional Complex Matrices	329
10.6	3D Complex HTs	332
10.7	Construction of (λ, μ) High-Dimensional Generalized Hadamard Matrices	335
	References	339
Chapter 11	Extended Hadamard Matrices	343
11.1	Generalized Hadamard Matrices	343
	11.1.1 Introduction and statement of problems	343

11.1.2	Some necessary conditions for the existence of generalized Hadamard matrices.....	346
11.1.3	Construction of generalized Hadamard matrices of new orders	347
11.1.4	Generalized Yang matrices and construction of generalized Hadamard matrices.....	350
11.2	Chrestenson Transform	351
11.2.1	Rademacher functions.....	351
11.2.2	Example of Rademacher matrices	353
11.2.2.1	Generalized Rademacher functions.....	354
11.2.2.2	The Rademacher–Walsh transforms.....	355
11.2.2.3	Chrestenson functions and matrices	357
11.3	Chrestenson Transform Algorithms.....	359
11.3.1	Chrestenson transform of order 3^n	359
11.3.2	Chrestenson transform of order 5^n	361
11.4	Fast Generalized Haar Transforms.....	365
11.4.1	Generalized Haar functions.....	365
11.4.2	2^n -point Haar transform.....	367
11.4.3	3^n -point generalized Haar transform.....	369
11.4.4	4^n -point generalized Haar transform.....	371
11.4.5	5^n -point generalized Haar transform.....	374
	References	379
Chapter 12 Jacket Hadamard Matrices		383
12.1	Introduction to Jacket Matrices	383
12.1.1	Example of jacket matrices	383
12.1.2	Properties of jacket matrices.....	385
12.2	Weighted Sylvester–Hadamard Matrices	389
12.3	Parametric Reverse Jacket Matrices	392
12.3.1	Properties of parametric reverse jacket matrices.....	394
12.4	Construction of Special-Type Parametric Reverse Jacket Matrices.....	399
12.5	Fast Parametric Reverse Jacket Transform.....	404
12.5.1	Fast 4×4 parametric reverse jacket transform.....	405
12.5.1.1	One-parameter case.....	405
12.5.1.2	Case of three parameters	407
12.5.2	Fast 8×8 parametric reverse jacket transform.....	409
12.5.2.1	Case of two parameters.....	409
12.5.2.2	Case of three parameters	409
12.5.2.3	Case of four parameters.....	411
12.5.2.4	Case of five parameters.....	413
12.5.2.5	Case of six parameters	414
	References	416

Chapter 13 Applications of Hadamard Matrices in Communication Systems	419
13.1 Hadamard Matrices and Communication Systems.....	419
13.1.1 Hadamard matrices and error-correction codes.....	419
13.1.2 Overview of Error-Correcting Codes.....	419
13.1.3 How to create a linear code	425
13.1.4 Hadamard code.....	427
13.1.5 Graphical representation of the (7, 3, 4) Hadamard code ..	431
13.1.6 Levenshtein constructions.....	431
13.1.7 Uniquely decodable base codes	435
13.1.8 Shortened code construction and application to data coding and decoding.....	438
13.2 Space–Time Codes from Hadamard Matrices.....	440
13.2.1 The general wireless system model.....	440
13.2.2 Orthogonal array and linear processing design	442
13.2.3 Design of space–time codes from the Hadamard matrix ...	444
References	445
Chapter 14 Randomization of Discrete Orthogonal Transforms and Encryption	449
14.1 Preliminaries.....	450
14.1.1 Matrix forms of DHT, DFT, DCT, and other DOTs.....	450
14.1.2 Cryptography	452
14.2 Randomization of Discrete Orthogonal Transforms	453
14.2.1 The theorem of randomization of discrete orthogonal transforms.....	454
14.2.2 Discussions on the square matrices P and Q	454
14.2.3 Examples of randomized transform matrix M_s	456
14.2.4 Transform properties and features	459
14.2.5 Examples of randomized discrete orthogonal transforms..	459
14.3 Encryption Applications	460
14.3.1 1D data encryption	462
14.3.2 2D data encryption and beyond	463
14.3.3 Examples of image encryption.....	464
14.3.3.1 Key space analysis.....	464
14.3.3.2 Confusion property.....	465
14.3.3.3 Diffusion property	466
References	470
Appendix	475
A.1 Elements of Matrix Theory.....	475
A.2 First Rows of Cyclic Symmetric Williamson-Type Matrices of Order n , $n = 3, 5, \dots, 33, 37, 39, 41, 43, 49, 51, 55, 57, 61, 63$ [2]....	479

A.3	First Block Rows of the Block-Cyclic, Block-Symmetric (BCBS) Williamson–Hadamard Matrices of order $4n$, $n = 3, 5, \dots, 33, 37, 39, 41, 43, 49, 51, 55, 57, 61, 63$ [2].....	484
A.4	First Rows of Cyclic Skew-Symmetric Williamson-Type Matrices of Order n , $n = 3, 5, \dots, 33, 35$	487
A.5	First Block Rows of Skew-Symmetric Block Williamson–Hadamard Matrices of Order $4n$, $n = 3, 5, \dots, 33, 35$	494
	References	498
	Index	499

Preface

The Hadamard matrix and Hadamard transform are fundamental problem-solving tools used in a wide spectrum of scientific disciplines and technologies including communication systems, signal and image processing (signal representation, coding, filtering, recognition, and watermarking), and digital logic (Boolean function analysis and synthesis, and fault-tolerant system design). They are thus a key component of modern information technology. In communication, the most important applications include error-correcting codes, spreading sequences, and cryptography. Other relevant applications include analysis of stock market data, combinatorics, experimental design, quantum computing, environmental monitoring, and many problems in chemistry, physics, optics, and geophysical analysis.

Hadamard matrices have attracted close attention in recent years, owing to their numerous known and new promising applications. In 1893, Jacques Hadamard conjectured that for any integer m divisible by 4, there is a Hadamard matrix of the order m . Despite the efforts of a number of individuals, this conjecture remains unproved, even though it is widely believed to be true. Historically, the problem goes back to James Joseph Sylvester in 1867.

The purpose of this book is to bring together different topics concerning current developments in Hadamard matrices, transforms, and their applications. *Hadamard Transforms* distinguishes itself from other books on the same topic because it achieves the following:

- Explains the state of our knowledge of Hadamard matrices, transforms, and their important generalizations, emphasizing intuitive understanding while providing the mathematical foundations and description of fast transform algorithms.
- Provides a concise introduction to the theory and practice of Hadamard matrices and transforms. The full appearance of this theory has been realized only recently, as the authors have pioneered, for example, multiplication theorems, $4m$ -point fast Hadamard transform algorithms, and decomposition Hadamard matrices by vectors.
- Offers a comprehensive and unified coverage of Hadamard matrices with a balance between theory and implementation. Each chapter is designed to begin with the basics of the theory, progressing to more advanced topics, and then discussing cutting-edge implementation techniques.

- Covers a wide range of problems of these matrices/transforms, formulates open questions, and points the way to possible new developments in the field.
- Builds a complete background on the Hadamard matrices for professionals and students.
- A chapter (written by Yue Wu, Joseph P. Noonan, and Sos Agaian) featuring a never-before-published general method for improving encryption systems.

This book is suitable for a wide variety of audiences, including graduate students in electrical and computer engineering, mathematics, or computer science. *Hadamard Transforms* will prepare the reader for further exploration and support aspiring researchers in the field. The reader is not presumed to have a sophisticated mathematical background, but some mathematical familiarity is helpful.

Sos Agaian
Hakob Sarukhanyan
Karen Egiazarian
Jaakko Astola
July 2011

Acknowledgments

This work has been achieved through long-term research collaboration among the following three institutions:

- Department of Electrical Engineering, University of Texas at San Antonio, USA.
- Institute for Informatics and Automation Problems of the National Academy of Sciences of Armenia (IIAP NAS RA), Yerevan, Armenia.
- The Tampere International Center for Signal Processing (TICIP), Tampere University of Technology, Tampere, Finland.

This work is partially supported by NSF Grant No. HRD-0932339. The authors are grateful to these organizations.

Special thanks are due to Mrs. Zoya Melkumyan (IIAP) and to Mrs. Pirko Ruotsalainen (TICIP), of the Official for International Affairs of TICSP, for great help in organizing several of S. Aghaian's and H. Sarukhanyan's trips and visits to Finland. Thanks go to Mrs. Carol Costello for her careful editing of our manuscript. We also express our appreciation to Tim Lamkins, Dara Burrows, Gwen Weerts, Beth Kelley, and Scott McNeill, members of the SPIE editing team.