Hadamard Transforms

Hadamard Transforms

Sos Agaian

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 Agaian ... [et al.].
p. cm. – (Press monograph ; 207)
Includes bibliographical references and index.
ISBN 978-0-8194-8647-9
1. Hadamard matrices. I. Agaian, 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

Printed in the United States of America.

First printing

Contents

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. Agaian'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.