Orthogonal Designs

Jennifer Seberry

Orthogonal Designs

Hadamard Matrices, Quadratic Forms and Algebras

Springer

Jennifer Seberry
School of Computing and Information
Technology
University of Wollongong
Wollongong, NSW
Australia

ISBN 978-3-319-59031-8 ISBN 978-3-319-59032-5 (eBook)
DOI 10.1007/978-3-319-59032-5

Library of Congress Control Number: 2017945720

Original publication: "Orthogonal Designs: Hadamard matrices and quadratic forms" - A.V. Geramita, J. Seberry. 1979. Marcel Deckker Press - Taylor & Francis, US.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is dedicated, with the greatest respect, to Anthony V Geramita who has now gone to the Erdos' great SF. I thank Joan Geramita, his friend, colleague and heir, for permission to use Tony's work in this updated volume.

Preface

Problems concerned with the structure and existence of various kinds of matrices with elements from 0,1,-1, for example, Hadamard matrices and their generalization to weighing matrices, have long been of interest to workers in combinatorics and also applied statisticians, coding theorists, signal processors and other applied mathematicians. A first volume, "Orthogonal Designs: quadratic forms and Hadamard matrices" (Ed 1), was written jointly by Anthony V. Geramita and Jennifer Seberry and published by Marcel Dekker in 1979, but never reprinted. This 1979 volume, devoted to a ground-breaking approach, illuminated the connections between these various kinds of matrices and exposed new connections with several other areas of mathematics. The current volume, "Orthogonal Designs: Hadamard matrices, quadratic forms and algebras", is the revision and update of the initial volume created using research theses and papers written in the intervening years. This more recent research has led to new ideas for many areas of mathematics, signal processing and non-deterministic computer programming in computational mathematics. These approaches are through the investigation of orthogonal designs: roughly speaking, special matrices with indeterminate entries.

Originally this subject had been discussed in our research papers and those of our colleagues and students. The discovery of the intimate relationship between orthogonal designs and rational quadratic forms had not appeared in print before 1973. The finding of numerous constructions and interesting objects that appeared fundamental to the study of Hadamard matrices (and their generalizations) finally prompted Geramita and Seberry to look afresh at the work that had already appeared. They recast their work and their collaborators and students in the light of their new discoveries. This present updated and new work continues the previous book and introduces more recent material by collaborators, colleagues and students. It leads to new algebras, techniques and existence results.

As will be clear in the text, orthogonal designs is a heavy "borrower" of mathematics. The reader will find us using results from, for example, algebraic number theory, quadratic forms, difference sets, representation theory, coding theory, finite geometry, elementary number theory, cyclotomy, the theory of computation and signal processing. The reader is not expected to be conversant with all these areas; the material is presented in such a way that even the novice to these areas will understand why and how we intend to use the results stated, even if the proofs in some cases remain a mystery. In those cases where detailed explanation would take too long, references are given so the interested reader can fill out their background. Thus the original volume and this volume can be profitably read both by experts and by people new to this area of discrete mathematics and combinatorics.

To dispel any notion that this book closes the area for further research, many problems are highlighted, all unsolved, and directions in which further research is possible are suggested. These problems vary in depth: some are seemingly very simple, others are major.

Some comments on how this volume is organized: the organization is, in part, directed by the Janus-like features of the study. In the first three chapters, which largely remain untouched and are heavily underpinned by the farsighted work of Anthony V. Geramita, the nature of the problem at hand is described, and some remarks made on the ingredients of a solution. After some preliminaries, a rather deep foray is made into the algebra side of the question. In broad terms, the algebra there described allows us to identify the first set of non-trivial necessary conditions on the problem of existence of orthogonal designs. Chapter 4 concentrates, and with the necessary conditions as a guide, on attempts to satisfy these conditions. Many different methods of construction are described and analysed. Chapter 5 focusses on one of these construction methods and analyses it in detail, both algebraically and combinatorially. Here again, the interplay between classical algebra and combinatorics is shown to have striking consequences. Chapter 6 deeply studies two construction methods introduced but not analysed in the original book. The result is new algebras which have been developed to encompass these combinatorial concepts. Chapter 7 deviates to give some of the theory and existence results for areas of number theory and discrete applied mathematics which have proved, over the past forty to fifty years, to have been somewhat forgotten by those not studying orthogonal designs. In Chapter 8 a very strong non-existence theorem for orthogonal designs is proved. The “Asymptotic Hadamard Existence Theorem” and related wonderful asymptotic consequences and questions, which are central to Chapter 9, are due to a number of authors. Chapter 10 reminds us that we have not finished with number theoretic consequences and other combinatorial features of orthogonal designs by commencing the study of non-real fields. Finally, in the Appendices, we tabulate numerous calculations we have made in specific orders.

Acknowledgements

No book this size could be the child of one or two parents. Many people are owed a debt of deep gratitude. For the original book Dan Shapiro (Ohio State) helped immensely with his work on similarities. The 1970's students Peter Robinson (ANU, Canberra), Peter Eades (ANU, Canberra) and Warren Wolfe (Queens', Kingston) had major input; the 1980's students of Seberry, Deborah J. Street (Sydney), Warwick de Launey (Sydney) and Humphrey Gastineau-Hills (Sydney), and the 2000's students Chung Le Tran (Wollongong) and Ying Zhao (Wollongong) have contributed conspicuously to the volume. Many, many colleagues such as Marilena Mitrouli (Athens), Christos Koukouvinos (NTUA, Athens) and his students Stelios Georgiou and Stella Stylianou, Hadi Kharghani (Lethbridge), Wolf Holzmann (Lethbridge), Rob Craigen (Winnipeg), Ilias Kotsireas (WLU), Dragomir Đoković (Waterloo), Sarah Spence Adams (Olin, Boston), Behruz Tayfeh-Rezaie (IPM, Tehran) and Ebrahim Ghaderpour (York, Toronto) have helped shape and correct our work. I acknowledge that at times I might have written utter rubbish without their knowledge and thoughts. I leave writing this book knowing it is an unfinished work, knowing that I have included many errors large and small. I acknowledge the generous proofing help for the original volume by Joan Geramita and Chuck Weibel. I acknowledge the LaTeXing proofing, and exceptional research assistance given me over the past ten years by Max Norden. I came to today with the help of the University of Wollongong Library and the provision of an office to me as Emeritus Professor.

From the original preface "Finally, a word of our experience writing this book. We approached the problems herein from quite different backgrounds. It became evident that Geramita was more interested in the connections with algebra, while Seberry was more interested in actually making the objects that could be made. The inevitable tensions that arise from these differing viewpoints (will), we hope, make this book more interesting to read."

Wollongong, Australia *Jennifer Seberry*
November 2016

Contents

About the Author

Emeritus Professor Jennifer Seberry is an Australian cryptographer, mathematician, and computer scientist, now at the University of Wollongong. A graduate of UNSW and LaTrobe, she has taught at the Universities of Newcastle, Sydney, UNSW (ADFA) and Wollongong. Her areas of research include discrete and combinatorial mathematics, Hadamard matrices and bent functions for cryptology, and orthogonal designs. She has published over 400 papers and 7 books. She was the first person in Australia to teach computer security to university students. She is highly respected and has been made a Fellow of the International Association for Cryptologic Research and a Chartered Mathematician by the Institute of Mathematics and its Applications.

List of Tables

List of Figures