Combinatorial Designs

Springer
New York
Berlin
Heidelberg
Hong Kong
London
Milan
Paris
Tokyo

Combinatorial Designs

Constructions and Analysis

Springer

Douglas R. Stinson
School of Computer Science
University of Waterloo
Waterloo ON N2L 3G1
Canada
dstinson@waterloo.ca

Library of Congress Cataloging-in-Publication Data
Stinson, Douglas R. (Douglas Robert), 1956–
Combinatorial designs : constructions and analysis / Douglas R. Stinson.
p. cm.
Includes bibliographical references and index.
ISBN 0-387-95487-2 (acid-free paper)
1. Combinatorial designs and configurations. I. Title
QA166.25.S75 2003
511′.6—dc21 2003052964

ISBN 0-387-95487-2 Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 10826487

Typesetting: Pages were created by the author using the Springer LaTeX2e with svmono and author macros.

www.springer-ny.com

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

To Ron Mullin, who taught me design theory

Foreword

The evolution of combinatorial design theory has been one of remarkable successes, unanticipated applications, deep connections with fundamental mathematics, and the desire to produce order from apparent chaos. While some of its celebrated successes date from the eighteenth and nineteenth centuries in the research of Euler, Kirkman, Cayley, Hamilton, Sylvester, Moore, and others, not until the twentieth century did the study of combinatorial designs emerge as an academic subject in its own right. When Fisher and his colleagues developed the mathematics of experimental design in the 1920s, combinatorial design theory was born as a field intimately linked to its applications. Beginning in the 1930s, Bose and his school laid the foundations, embedding the nascent field firmly as a mathematical discipline by developing deep connections with finite geometry, number theory, finite fields, and group theory; however, Bose accomplished much more. His foundation entwined deep mathematics with its applications in experimental design and in recreational problems and anticipated its fundamental importance in the theory of error-correcting codes.

The rapid advances in design theory can be attributed in large degree to its impetus from applications in coding theory and communications and its continued deep interactions with geometry, algebra, and number theory. The last fifty years have witnessed not only the emergence of certain combinatorial designs (balanced incomplete block designs, Hadamard matrices, pairwise balanced designs, and orthogonal arrays, for example) as central, but also powerful combinatorial and computational techniques for their construction. Indeed the field grew so far and so fast that its historical connection to applications was strained.

Yet, in the last twenty years, combinatorial design theory has emerged again as a field rich in current and practical applications. The fundamental connections with algebra, number theory, and finite geometry remain and flourish. The applications in experimental design and coding theory have developed a breadth and depth that defy brief explanation. Yet combinatorial design theory has matured into more than this through applications in

cryptography, optical communications, storage system design, communication protocols, algorithm design and analysis, and wireless communications, to mention just a few areas.

Combinatorial design theory is mature and widely applied today because it has respected and advanced its mathematical heritage while finding genuine new applications. I am honored to write this foreword for two reasons. Doug Stinson has for twenty-five years been the epitome of a researcher and expositor who has advanced combinatorial design theory as a marriage of mathematics and applications. But more than that, the book you hold in your hands presents design theory as a seamless interaction of deep mathematics and challenging applications. By providing an accessible introduction, it serves as an invitation to those in applications areas to appreciate and employ beautiful mathematics and concurrently invites mathematicians to learn from the applications themselves.

In which directions will combinatorial design theory evolve in the next century? We cannot yet know. We can know, however, that new mathematical truths will be found and that unanticipated applications will arise. Our challenge is to seek both and to know that each profits from the other.

Phoenix, Arizona
April, 2003

Charles J. Colbourn

Preface

Overview and Goals

Combinatorial design theory is one of the most beautiful areas of mathematics. Design theory has its roots in recreational mathematics, but it evolved in the twentieth century into a full-fledged mathematical discipline with diverse applications in statistics and computer science. The fundamental problems in design theory are simple enough that they can be explained to nonmathematicians, yet the solutions of those problems have involved the development of innovative new combinatorial techniques as well as ingenious applications of methods from other areas of mathematics such as algebra and number theory. Many classical problems remain unsolved to this day as well.

This book is intended primarily to be a textbook for study at the senior undergraduate or beginning graduate level. Courses in mathematics or computer science can be based on this book. Regardless of the audience, however, it requires a certain amount of "mathematical maturity" to study design theory. The main technical prerequisites are some familiarity with basic abstract algebra (group theory, in particular), linear algebra (matrices and vector spaces), and some number-theoretic fundamentals (e.g., modular arithmetic and congruences).

Topic Coverage and Organization

The first seven chapters of this book provide a thorough treatment of the classical core of the subject of combinatorial designs. These chapters concern symmetric BIBDs, difference sets, Hadamard matrices, resolvable BIBDs, Latin squares, and pairwise balanced designs. A one-semester course can cover most of this material. For example, when I have taught courses on designs, I have based my lectures on material selected from the following chapters and sections:

- Chapter 1: Sections 1.1–1.3, Section 1.4 (optional), Sections 1.5–1.6
- Chapter 2: Sections 2.1–2.4
- Chapter 3: Sections 3.1–3.4
- Chapter 4: Sections 4.1–4.4, Section 4.5 (optional), Section 4.6
- Chapter 5: Sections 5.1–5.2, Section 5.3 (optional)
- Chapter 6: Sections 6.1, Section 6.2 (optional), Sections 6.3–6.8
- Chapter 7: Sections 7.1–7.3

There are many variations possible, of course. Typically, I would provide a complete proof of the Bruck-Ryser-Chowla Theorem or the Multiplier Theorem, but not both. It is possible to omit Wilson's Construction for MOLS in order to spend more time on pairwise balanced designs. Another option is to include the optional Section 6.2 and omit some of the material in Chapter 7. Yet another possibility is to present an introduction to t-designs (incorporating some material from Chapter 9, Sections 9.1 and 9.2) and delete some of the optional sections listed above.

More advanced or specialized material is covered in the last four chapters as well as in some later sections of the first seven chapters. The main topics in the last four chapters are minimal pairwise balanced designs, t-designs, orthogonal arrays and codes, and four selected applications of designs (in the last chapter).

Key Features

There are several features of this book that will make it useful as a textbook. Complete, carefully written proofs of most major results are given. There are many examples provided throughout in order to illustrate the definitions, concepts, and theorems. Numerous and varied exercises are provided at the end of each chapter. As well, certain mathematical threads flow through this book:

- The linear algebraic method of proving Fisher's Inequality reappears several times.
- The theme of Boolean functions is introduced in the study of bent functions and revisited in the discussion of Reed-Muller codes and a brief treatment of resilient functions.
- The use of permutation groups as a construction technique is pervasive.
- Elegant combinatorial arguments are used in many places in preference to alternative proofs that employ heavier mathematical machinery.
- Finite fields are used throughout the book. For this reason, some background material on finite fields is summarized in an Appendix. However, another option for an instructor is to specialize constructions utilizing finite fields $\mathbb{F}_q$ to the more familiar fields $\mathbb{Z}_p$, where p is a prime.

As mentioned earlier, there are a variety of advanced or specialized topics that are discussed in the book. Highlights include the following:

- regular Hadamard matrices and excess of Hadamard matrices;
- bent functions;
- bounds and constructions for minimal pairwise balanced designs;
- the Ryser-Woodall Theorem;
- constructions and bounds for t-wise balanced designs, including a proof of the Kramer Conjecture;
- a survey of the combinatorial connections between orthogonal arrays, codes, and designs;
- constructions and bounds for various classes of optimal codes and orthogonal arrays;
- Reed-Muller codes;
- resilient functions;
- four selected applications of designs: authentication codes, threshold schemes, group testing, and two-point sampling.

It must be recognized that design theory is an enormous subject, and any choice of optional material in a 300 page book is dependent on the whim of the author! Thus there are many interesting or important areas of design theory that are not discussed in the book. I hope, however, that readers of the book will find a fascinating mix of topics that serve to illustrate the breadth and beauty of design theory.

Audience

As mentioned above, this book is primarily intended to be a textbook. In addition, all of the material in this book is suitable for self-study by graduate students, who will find it provides helpful background information concerning research topics in design theory. Researchers may also find that some of the sections on advanced topics provide a useful reference for material that is not easily accessible in textbook form.

Acknowledgments

I have benefitted from the suggestions, comments and encouragement of many people while this book was being written. In particular, I would like to thank Charlie Colbourn, Don Kreher, and Brett Stevens. Special thanks goes to Dameng Deng for his help with proofreading. Also, I appreciate the assistance and advice of Wayne Yuhasz and Wayne Wheeler from Springer during this project.

Waterloo, Ontario, Canada *Douglas R. Stinson*
July, 2003

Contents