LONDON MATHEMATICAL SOCIETY STUDENT TEXTS

Managing editor: Dr C.M. Series, Mathematics Institute
University of Warwick, Coventry CV4 7AL, United Kingdom

1 Introduction to combinators and λ-calculus, J.R. HINDLEY & J.P. SELDIN
2 Building models by games, WILFRID HODGES
3 Local fields, J.W.S. CASSELS
4 An introduction to twistor theory: Second edition, S.A. HUGGETT & K.P. TOD
5 Introduction to general relativity, L.P. HUGHSTON & K.P. TOD
6 Lectures on stochastic analysis: diffusion theory, DANIEL W. STROOCK
7 The theory of evolution and dynamical systems, J. HOFBAUER & K. SIGMUND
8 Summing and nuclear norms in Banach space theory, G.J.O. JAMESON
9 Automorphisms of surfaces after Nielsen and Thurston, A. CASSON & S. BLEILER
10 Nonstandard analysis and its applications, N. CUTLAND (ed)
11 Spacetime and singularities, G. NABER
12 Undergraduate algebraic geometry, MILES REID
13 An introduction to Hankel operators, J.R. PARTINGTON
14 Combinatorial group theory: a topological approach, DANIEL E. COHEN
15 Presentations of groups, D.L. JOHNSON
16 An introduction to noncommutative Noetherian rings, K.R. GOODEARL & R.B. WARFIELD, JR.
17 Aspects of quantum field theory in curved spacetime, S.A. FULLING
18 Braids and coverings: selected topics, VAGN LUNDSGAARD HANSEN
19 Steps in commutative algebra, R.Y. SHARP
20 Communication theory, C.M. GOLDIE & R.G.E. PINCH
21 Representations of finite groups of Lie type, FRANÇOIS DIGNE & JEAN MICHEL
22 Designs, graphs, codes, and their links, P.J. CAMERON & J.H. VAN LINT
23 Complex algebraic curves, FRANCES KIRWAN
24 Lectures on elliptic curves, J.W.S. CASSELS
25 Hyperbolic geometry, BIRGER IVERSEN
26 An introduction to the theory of L-functions and Eisenstein series, H. HIDA
27 Hilbert Space: compact operators and the trace theorem, J.R. RETHERFORD
28 Potential theory in the complex plane, T. RANSFORD
29 Undergraduate commutative algebra, M. REID
32 Lectures on Lie Groups and Lie Algebras, R. CARTER, G. SEGAL & I. MACDONALD
33 A primer of algebraic *D*-modules, S.C. COUTINHO

London Mathematical Society Student Texts 22

Designs, Graphs, Codes and their Links

P. J. Cameron
Professor of Mathematics, Queen Mary and Westfield College, London

and

J. H. van Lint
Professor of Mathematics, Eindhoven University of Technology

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1991
Reprinted 1996

Library of Congress cataloging in publication data available

A catalogue record for this book is available from the British Library

ISBN 0 521 41325 7 hardback
ISBN 0 521 42385 6 paperback

Transferred to digital reprinting 2000

Contents

Preface

The three subjects of this book all began life in the provinces of applicable mathematics. Design theory originated in statistics (its name reflects its initial use, in experimental design); codes in information transmission; and graphs in the modelling of networks of a very general kind (in the first instance, the bridges of Königsberg). All three have since become part of mainstream discrete mathematics.

We have not tried to write a textbook on three individual topics. Instead, our goal is more limited: we want to explore some of the ways in which the three topics have interacted with each other, with results and methods from one area being applied in another. Indeed, we believe that discrete mathematics is better defined by its methods than by its subject-matter, and our approach reflects this.

The book has its origins in the notes of two series of lectures given by the authors at Westfield College, London, at the invitation of Dan Hughes. The audience at those lectures consisted of design theorists, and our job was to show them that graphs and codes could be useful to them. The notes subsequently appeared in the London Mathematical Society Lecture Note Series in 1975, and in a considerably revised form in 1980. We tried then to make the notes accessible to a wider audience by adding an introductory chapter on design theory.

In the intervening decade, we have become aware that a number of students used the book as a textbook. Their task was not made easier by the 'research notes' style in which many assertions are left without proof. Accordingly, when David Tranah approached us about a new revision, we decided to re-write the book completely, turning it into a textbook. We have expanded considerably the chapters on design theory, strongly regular graphs, and codes; we have, wherever possible, included proofs of our assertions, and avoided words like 'clearly ...'; and we have added a number of exercises, with hints where appropriate.

In addition, we have brought the material up-to-date, with a number of new topics (including graphs with least eigenvalue -2 and their connection with root systems, strongly regular graphs with strongly regular subconstituents, and expanded treatments of two-graphs, partial geometries, Preparata and Kerdock codes, two-weight projective codes, P- and Q-polynomial association schemes, etc.), as well as smaller additions.

We are grateful to large numbers of students and colleagues for bringing errors and difficulties in the previous version to our attention, or for commenting on draft chapters of this book. Especially, Rosemary Bailey, Frank De Clerck, Jon Hall, and Jef Thas have given us great help.

We have used electronic mail to send the manuscript between one another, plain TEX for the typesetting, and the laser printer in the School of Mathematical Sciences at Queen Mary and Westfield College, London, to produce camera-ready copy.

As we said, this is not a textbook on graphs, codes, or designs — our treatment of these is mostly limited to the particular interconnections we discuss — and our readers may require more extended treatments. We refer them to Hughes and Piper (1985) for designs, Beineke and Wilson (1978), (1983) for graphs, and van Lint (1982) for codes. Though we give many references, it is not compulsory to read all these!

We assume a background of undergraduate algebra. The following list of results includes most of what is needed. These results can be found in any good algebra textbook. We give references to the two-volume *Algebra*, by P. M. Cohn (1974), (1977).

- Finite fields have prime power order. For each $q = p^d$ (with p prime and $d > 0$), there is a unique field of order q, up to isomorphism (the Galois field). Its multiplicative group is cyclic of order $q - 1$, and its automorphism group is cyclic of order d. (Cohn (1977), p. 195.)
- For any real symmetric matrix A, there is an orthonormal basis of $\mathbf{R}^n$ consisting of eigenvectors of A. Equivalently, there is an orthogonal matrix P such that $PAP^\top$ is diagonal. (Cohn (1974), p. 203.)
- For any $m \times n$ integer matrix A, there are integer matrices P and Q with determinant 1 such that $PAQ = \left(\begin{smallmatrix} D & O \\ O & O \end{smallmatrix}\right)$, where $D = \operatorname{diag}(d_1, \ldots, d_r)$, the d_i being non-zero integers satisfying $d_1 | d_2 | \ldots | d_r$. (This is the Smith normal form of A; the numbers d_i are the elementary divisors of A.) (Cohn (1974), p. 279.)
- The polynomial ring over a field, or any quotient of this ring, is a principal ideal domain. (Cohn (1974), pp. 134, 276.)
- If A is a finite abelian group, then the group of characters of A (homomorphisms to the multiplicative group of non-zero complex numbers) is isomorphic to A. (Cohn (1974), p. 243; (1977), p. 163.) (In fact, we only use this for groups A which are given as direct sums of cyclic groups, so the 'Fundamental Theorem of Abelian Groups' is not required.)
- We also assume familiarity with the concepts of a group and the action of a group on a set, and a few specific groups (Cohn (1974), p. 47.)

On the other hand, we have made no assumptions about prerequisites in discrete mathematics. Usually, what we need is developed in the text; but we have included an account of the Principle of Inclusion and Exclusion as an appendix to Chapter 1. (See Hall (1986) for further discussion.)

Notation and terminology

Our terminology is mostly standard, with a few exceptions. In particular, we use the term 'square 2-design' for what is usually called 'symmetric design', '$(0,k)$-set' for 'maximal k-arc', and 'ball' for 'sphere'. Our reasons for these decisions are explained in the text.

In many instances, the symbols commonly used for parameters of designs, graphs, geometries, etc. conflict with one another. There is no simple solution to this, and we have been deliberately inconsistent, in the interests of clarity. The reader's attention is drawn to this whenever it occurs.

We use F_q to denote the Galois field with q elements, where q is a prime power. (This field is often called $\mathrm{GF}(q)$.) Vectors, over a finite field or the real numbers, are written in bold face.

If $\mathbf{u}$ and $\mathbf{v}$ are vectors in some vector space, then
$\langle \mathbf{u}, \mathbf{v} \rangle$ denotes their dot product;
$[\mathbf{u}, \mathbf{v}]$ denotes the subspace they span;
$(\mathbf{u}, \mathbf{v})$ denotes simply the ordered pair.
The square brackets for span are also used for arbitrary sets of vectors.

An n-tuple of scalars in round brackets denotes a row vector, in the usual way. Matrices are denoted by capital letters, and the transpose of A is written $A^\top$. This notation is also extended to denote 'duals' of other algebraic or combinatorial objects (for example, designs), as explained in the text.