LONDON MATHEMATICAL SOCIETY STUDENT TEXTS

42 Equilibrium states in ergodic theory, GERHARD KELLER
43 Fourier analysis on finite groups and applications, AUDREY TERRAS
44 Classical invariant theory, PETER J. OLVER
45 Permutation groups, PETER J. CAMERON
47 Introductory lectures on rings and modules. JOHN A. BEACHY
48 Set theory, ANDRÁS HAJNAL & PETER HAMBURGER. Translated by ATTILA MATE
49 An introduction to K-theory for C*-algebras, M. RØRDAM, F. LARSEN & N. J. LAUSTSEN
50 A brief guide to algebraic number theory, H. P. F. SWINNERTON-DYER
51 Steps in commutative algebra: Second edition, R. Y. SHARP
52 Finite Markov chains and algorithmic applications, OLLE HÄGGSTRÖM
53 The prime number theorem, G. J. O. JAMESON
54 Topics in graph automorphisms and reconstruction, JOSEF LAURI & RAFFAELE SCAPELLATO
55 Elementary number theory, group theory and Ramanujan graphs, GIULIANA DAVIDOFF, PETER SARNAK & ALAIN VALETTE
56 Logic, induction and sets, THOMAS FORSTER
57 Introduction to Banach algebras, operators and harmonic analysis, GARTH DALES *et al*.
58 Computational algebraic geometry, HAL SCHENCK
59 Frobenius algebras and 2-D topological quantum field theories, JOACHIM KOCK
60 Linear operators and linear systems, JONATHAN R. PARTINGTON
61 An introduction to noncommutative Noetherian rings: Second edition, K. R. GOODEARL & R. B. WARFIELD, JR
62 Topics from one-dimensional dynamics, KAREN M. BRUCKS & HENK BRUIN
63 Singular points of plane curves, C. T. C. WALL
64 A short course on Banach space theory, N. L. CAROTHERS
65 Elements of the representation theory of associative algebras I, IBRAHIM ASSEM, DANIEL SIMSON & ANDRZEJ SKOWROŃSKI
66 An introduction to sieve methods and their applications, ALINA CARMEN COJOCARU & M. RAM MURTY
67 Elliptic functions, J. V. ARMITAGE & W. F. EBERLEIN
68 Hyperbolic geometry from a local viewpoint, LINDA KEEN & NIKOLA LAKIC
69 Lectures on Kähler geometry, ANDREI MOROIANU
70 Dependence logic, JOUKU VÄÄNÄNEN
71 Elements of the representation theory of associative algebras II, DANIEL SIMSON & ANDRZEJ SKOWROŃSKI
72 Elements of the representation theory of associative algebras III, DANIEL SIMSON & ANDRZEJ SKOWROŃSKI
73 Groups, graphs and trees, JOHN MEIER
74 Representation theorems in Hardy spaces, JAVAD MASHREGHI
75 An introduction to the theory of graph spectra, DRAGOŠ CVETKOVIĆ, PETER ROWLINSON & SLOBODAN SIMIĆ
76 Number theory in the spirit of Liouville, KENNETH S. WILLIAMS
77 Lectures on profinite topics in group theory, BENJAMIN KLOPSCH, NIKOLAY NIKOLOV & CHRISTOPHER VOLL
78 Clifford algebras: an introduction, D. J. H. GARLING
79 Introduction to compact Riemann surfaces and dessins d'enfants, ERNESTO GIRONDO & GABINO GONZÁLEZ-DIEZ
80 The Riemann hypothesis for function fields, MACHIEL VAN FRANKENHUIJSEN
81 Number theory, Fourier analysis and geometric discrepancy, GIANCARLO TRAVAGLINI

London Mathematical Society Student Texts 82

Finite Geometry and Combinatorial Applications

SIMEON BALL
Universitat Politècnica de Catalunya, Barcelona

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107518438

First published 2015

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

Library of Congress Cataloging-in-Publication data
Ball, Simeon (Simeon Michael)
Finite geometry and combinatorial applications / Simeon Ball,
Universitat Politècnica de Catalunya, Barcelona.
pages cm. – (London Mathematical Society student texts ; 82)
Includes bibliographical references and index.
ISBN 978-1-107-10799-1 (Hardback : alk. paper) –
ISBN 978-1-107-51843-8 (Paperback : alk. paper)
1. Finite geometries. 2. Combinatorial analysis. I. Title.
QA167.2.B35 2015
516´.11–dc23 2015009563

ISBN 978-1-107-10799-1 Hardback
ISBN 978-1-107-51843-8 Paperback

Contents

Preface

This book is essentially a text book that introduces the geometrical objects which arise in the study of vector spaces over finite fields. It advances rapidly through the basic material, enabling the reader to consider the more interesting aspects of the subject without having to labour excessively. There are over a hundred exercises which contain a lot of content not included in the text. This should be taken into consideration and even though one may not wish to try to solve the exercises themselves, they should not be ignored. There are detailed solutions provided to all the exercises.

The first four chapters treat the algebraic and geometric aspects of finite vector spaces. The following three chapters consist of combinatorial applications. There is a chapter containing a brief treatment of applications to groups, real geometry, codes, graphs, designs and permutation polynomials. Then there is a chapter that gives a more in-depth treatment of applications to extremal graph theory, specifically the forbidden subgraph problem, and then a chapter on maximum distance separable codes.

This book is self-contained in the sense that any theorem or lemma which is subsequently used is proven. The only exceptions to this are Bombieri's theorem and the Huxely–Iwaniec theorem concerning the distribution of primes, which are used in the chapter on the forbidden subgraph problem, the Hasse–Weil theorem, which is used to bound the number of points on a plane algebraic curve at the end of the chapter on maximum distance separable codes, and Hilbert's Nullstellensatz, which is used in the appendix on commutative algebra. Although there are almost no prerequisites, it would be helpful to have studied previously some basic algebra and linear algebra, since otherwise the first couple of chapters may appear somewhat brief. There are some theorems that are quoted without proof, but in all cases these appear at the end of some branch and are not built upon. There are some theorems whose proof appears

in Appendix B. This is done when the proof of some particular theorem may interrupt the flow of the book.

How to use this book if ...

... you are not teaching a course. For many readers a lot of the material in Chapter 1 and Chapter 2 will be familiar. However, some of the exercises, those relating to latin squares, semifields and spreads, may not be and are, although not generally essential, at least relevant to what appears in later chapters. For this reason they should not be overlooked. There is no need to read all the details of Chapter 3. It is enough to read as far as Theorem 3.6, choose one of the σ-sesquilinear forms to consider in more detail and Section 3.6. The central chapters of the book are Chapter 4 and Chapter 5.

... you are teaching a course. This book is not structured as lecture notes. However, there is plenty of material to plan a course, even within a pre-established syllabus. Note that a lot of the material is contained in exercises that, since the solutions are provided, can be explained as theorems in class. One could teach the following course.

(1) Latin squares. Definition and exercises from Chapter 1 and use these lectures to (re-)introduce the student to finite fields.
(2) Affine planes. Exercises in Chapter 4, use some as theorems and leave the rest as exercises.
(3) Projective planes. Text and exercises in Chapter 4, introducing example of $\mathrm{PG}_2(\mathbb{F}_q)$ and Desargues' theorem.
(4) Projective spaces. Use Chapter 4.
(5) Polar spaces. Sketch classification of σ-sesquilinear forms, i.e. Chapter 3 as far as Theorem 3.6 and sketch Section 3.6. Then Theorem 4.3.
(6) Quotient spaces. Section 4.3 and Section 4.4.
(7) Generalised polygons. Section 4.5.
(8) Ovals and ovoids. Section 4.8 and include Segre's theorem, Theorem 4.38.

One could then pick and choose from Chapter 5 and maybe Chapter 6. Although it may be disheartening to see a full set of solutions, many of the exercises can be easily adapted so that exercise sheets, which do not have solutions, can be compiled if necessary.

By no means do I consider the contents of this book to be an unbiased view of what finite geometry is. There are aspects of the subject that I have barely touched upon and some I have not mentioned at all. I have stuck, in the main part, to that which is of interest to me and that I feel confident enough to write about.

Notation

$\mathbb{C}$	the complex numbers.
$\mathrm{char}(\mathbb{F})$	the characteristic of the field $\mathbb{F}$.
$\det(u_1, \ldots, u_k)$	the determinant of the matrix whose ijth entry is the jth coordinate of u_i with respect to a canonical basis.
$\mathrm{ex}(n, H)$	the maximum number of edges a graph G with n vertices can have that contains no H as a subgraph.
$\mathbb{E}(X)$	the expectation of a random variable X.
$\mathbb{F}_q$	the finite field with q elements.
$\mathrm{Fix}(\sigma)$	the subfield fixed by the automorphism σ of a field.
$\gcd(a, b)$	the greatest common divisor of two positive integers a and b.
I_n	the $n \times n$ identity matrix.
$\mathrm{im}(\alpha)$	the image of the linear map α.
$\ker(\alpha)$	the kernel of the linear map α.
$\mathrm{H}_{k-1}(\mathbb{F})$	the hermitian polar space of rank r, where $k = 2r$ or $k = 2r + 1$.
$\mathbb{N}$	the set of positive integers.
Norm_σ	the norm map from a field to the subfield $\mathrm{Fix}(\sigma)$.
$\mathrm{PG}_{k-1}(\mathbb{F})$	the $(k-1)$-dimensional projective space over $\mathbb{F}$.
$\mathrm{Q}^+_{k-1}(\mathbb{F})$	the hyperbolic polar space of rank r, where $k = 2r$.
$\mathrm{Q}_{k-1}(\mathbb{F})$	the parabolic polar space of rank r, where $k = 2r + 1$.
$\mathrm{Q}^-_{k-1}(\mathbb{F})$	the elliptic polar space of rank r, where $k = 2r + 2$.
$\mathbb{R}$	the real numbers.
$\mathrm{Sym}(n)$	the symmetric group of permutations on the set $\{1, \ldots, n\}$.
Tr_σ	the trace map from a field to the subfield $\mathrm{Fix}(\sigma)$.
$\langle u_1, \ldots, u_r \rangle$	the subspace spanned by the vectors $u_1, \ldots, u_r$.
$U_1 + \cdots + U_r$	the sum of subspaces $U_1, \ldots, U_r$.

$U_1 \oplus \cdots \oplus U_r$	the direct sum of subspaces $U_1, \ldots, U_r$.
$U^\perp$	the orthogonal subspace of a subspace U, defined with respect to some σ-sesquilinear form.
$V(f)$	the algebraic variety defined by the polynomial f.
$\mathrm{V}_k(\mathbb{F})$	the k-dimensional vector space over $\mathbb{F}$.
$\mathrm{W}_{k-1}(\mathbb{F})$	the symplectic polar space of rank r, where $k = 2r$.
$\mathbb{Z}$	the set of integers.