

LONDON MATHEMATICAL SOCIETY STUDENT TEXTS

Managing Editor: Professor D. Benson,
 Department of Mathematics, University of Aberdeen, UK

- 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 & Assessment
 978-1-107-51843-8 — Finite Geometry and Combinatorial Applications
 Simeon Ball
 Frontmatter
[More Information](#)



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

© Simeon Ball 2015

This publication is in copyright. Subject to statutory exception and to the provisions
 of relevant collective licensing agreements, no reproduction of any part may take
 place without the written permission of Cambridge University Press & Assessment.

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

Cambridge University Press & Assessment has no responsibility for the persistence
 or accuracy of URLs for external or third-party internet websites referred to in this
 publication and does not guarantee that any content on such websites is, or will
 remain, accurate or appropriate.

Contents

	<i>Preface</i>	page ix
	<i>Notation</i>	xi
1	Fields	1
	1.1 Rings and fields	1
	1.2 Field automorphisms	6
	1.3 The multiplicative group of a finite field	9
	1.4 Exercises	10
2	Vector spaces	15
	2.1 Vector spaces and subspaces	15
	2.2 Linear maps and linear forms	17
	2.3 Determinants	19
	2.4 Quotient spaces	20
	2.5 Exercises	21
3	Forms	25
	3.1 σ -Sesquilinear forms	25
	3.2 Classification of reflexive forms	27
	3.3 Alternating forms	30
	3.4 Hermitian forms	34
	3.5 Symmetric forms	38
	3.6 Quadratic forms	40
	3.7 Exercises	47
4	Geometries	51
	4.1 Projective spaces	51
	4.2 Polar spaces	54
	4.3 Quotient geometries	60

4.4	Counting subspaces	61
4.5	Generalised polygons	65
4.6	Plücker coordinates	71
4.7	Polarities	74
4.8	Ovoids	76
4.9	Exercises	83
5	Combinatorial applications	93
5.1	Groups	93
5.2	Finite analogues of structures in real space	99
5.3	Codes	105
5.4	Graphs	109
5.5	Designs	114
5.6	Permutation polynomials	117
5.7	Exercises	120
6	The forbidden subgraph problem	124
6.1	The Erdős–Stone theorem	124
6.2	Even cycles	125
6.3	Complete bipartite graphs	130
6.4	Graphs containing no $K_{2,s}$	132
6.5	A probabilistic construction of graphs containing no $K_{t,s}$	134
6.6	Graphs containing no $K_{3,3}$	135
6.7	The norm graph	137
6.8	Graphs containing no $K_{5,5}$	140
6.9	Exercises	144
7	MDS codes	147
7.1	Singleton bound	147
7.2	Linear MDS codes	148
7.3	Dual MDS codes	151
7.4	The MDS conjecture	152
7.5	Polynomial interpolation	154
7.6	The A -functions	155
7.7	Lemma of tangents	157
7.8	Combining interpolation with the lemma of tangents	162
7.9	A proof of the MDS conjecture for $k \leq p$	164
7.10	More examples of MDS codes of length $q + 1$	165
7.11	Classification of linear MDS codes of length $q + 1$ for $k \leq p$	167
7.12	The set of linear forms associated with a linear MDS code	172

Contents

vii

7.13	Lemma of tangents in the dual space	174
7.14	The algebraic hypersurface associated with a linear MDS code	177
7.15	Extendability of linear MDS codes	182
7.16	Classification of linear MDS codes of length $q + 1$ for $k < c\sqrt{q}$	184
7.17	A proof of the MDS conjecture for $k < c\sqrt{q}$	189
7.18	Exercises	189
Appendix A	Solutions to the exercises	191
A.1	Fields	191
A.2	Vector spaces	200
A.3	Forms	206
A.4	Geometries	213
A.5	Combinatorial applications	229
A.6	The forbidden subgraph problem	233
A.7	MDS codes	238
Appendix B	Additional proofs	242
B.1	Probability	242
B.2	Fields	243
B.3	Commutative algebra	247
Appendix C	Notes and references	263
C.1	Fields	263
C.2	Vector spaces	264
C.3	Forms	264
C.4	Geometries	264
C.5	Combinatorial applications	266
C.6	The forbidden subgraph problem	269
C.7	MDS codes	270
C.8	Appendices	271
	<i>References</i>	272
	<i>Index</i>	282

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 $\text{PG}_2(\mathbb{F}_q)$ 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.
$\text{char}(\mathbb{F})$	the characteristic of the field \mathbb{F} .
$\det(u_1, \dots, u_k)$	the determinant of the matrix whose ij th entry is the j th coordinate of u_i with respect to a canonical basis.
$\text{ex}(n, H)$	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.
$\text{Fix}(\sigma)$	the subfield fixed by the automorphism σ of a field.
$\text{gcd}(a, b)$	the greatest common divisor of two positive integers a and b .
I_n	the $n \times n$ identity matrix.
$\text{im}(\alpha)$	the image of the linear map α .
$\ker(\alpha)$	the kernel of the linear map α .
$\text{H}_{k-1}(\mathbb{F})$	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 $\text{Fix}(\sigma)$.
$\text{PG}_{k-1}(\mathbb{F})$	the $(k - 1)$ -dimensional projective space over \mathbb{F} .
$\text{Q}_{k-1}^+(\mathbb{F})$	the hyperbolic polar space of rank r , where $k = 2r$.
$\text{Q}_{k-1}(\mathbb{F})$	the parabolic polar space of rank r , where $k = 2r + 1$.
$\text{Q}_{k-1}^-(\mathbb{F})$	the elliptic polar space of rank r , where $k = 2r + 2$.
\mathbb{R}	the real numbers.
$\text{Sym}(n)$	the symmetric group of permutations on the set $\{1, \dots, n\}$.
Tr_σ	the trace map from a field to the subfield $\text{Fix}(\sigma)$.
$\langle u_1, \dots, u_r \rangle$	the subspace spanned by the vectors u_1, \dots, u_r .
$U_1 + \dots + U_r$	the sum of subspaces U_1, \dots, U_r .

$U_1 \oplus \cdots \oplus U_r$	the direct sum of subspaces U_1, \dots, 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 .
$V_k(\mathbb{F})$	the k -dimensional vector space over \mathbb{F} .
$W_{k-1}(\mathbb{F})$	the symplectic polar space of rank r , where $k = 2r$.
\mathbb{Z}	the set of integers.