

Cambridge University Press

0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Frontmatter/Prelims

[More information](#)

**CAMBRIDGE TRACTS IN
MATHEMATICS**

General Editors

B. BOLLOBAS, P. SARNAK, C. T. C. WALL

103 Designs and their codes

Cambridge University Press

0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key

Frontmatter/Prelims

[More information](#)

E. F. ASSMUS, JR.

Department of Mathematics, Lehigh University

J. D. KEY

Department of Mathematical Sciences, Clemson University

Designs and their codes



Cambridge University Press

0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Frontmatter/Prelims

[More information](#)

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 10311-4211, USA
10 Stamford Road, Oakleigh, Victoria 3166, Australia

© E. F. Assmus Jr. & J. D. Key 1992

First published 1992

First published in paperback (with corrections) 1993

Library of Congress cataloguing in publication data available

British Library cataloguing in publication data available

ISBN 0 521 41361 3 hardback

ISBN 0 521 45839 0 paperback

Transferred to digital printing 2004

Preface

The aim of this book is to study applications of algebraic coding theory to the analysis and classification of designs. Designs are usually classified by their parameter sets, by their inclusion in infinite families, or according to the type of automorphism group they admit — or in other ways related to their geometric properties. Here we have tried to confront the following questions. To what extent can algebraic coding theory address classification questions concerning designs? Can it assist in their construction? Does it provide insight into the structure and nature of classes of designs? We have tried to outline ways in which these questions have been answered and to point to areas where coding theory can make a valuable contribution to design theory.

These matters occupy the last three chapters of the book; the first five chapters are of a background nature and form an introduction to both the theory of designs and algebraic coding theory. Although parts of these chapters are elementary we hope they will be of interest even to the expert. We have rethought much of the material and some of the development is new. We have not always given complete proofs and in several instances we have given no proof at all. On the other hand there are occasions where we have given more than one proof for the same result. Our guiding principle has been to use the proofs as didactic aids rather than verifications of the assertions; in particular, where the proof in the literature is clear and easily available but would add little to the exposition, we have omitted it.

We have included a glossary of terms and symbols that we hope will aid the expert who wishes to jump into one of the last three chapters without consulting the first five. Thus, for example, someone interested only in what coding theory might have to say about Hadamard matrices will be able to begin by reading Chapter 7 — using the glossary and index in the event that a concept or the notation is unfamiliar. Similarly, someone interested in projective planes — and their coding-theoretic habitat — ought to be able to go directly to Chapter 6 and the Steiner-system expert directly to Chapter 8.

The numbering is standard and is consecutive within sections: thus the third exercise of the second section of the first chapter is Exercise 1.2.3. The theorems, propositions, corollaries, lemmas and examples are similarly listed. In the **Bibliography** the abbreviations for the titles of journals are those used by *Mathematical Reviews*; the full journal title is given in the event *Mathematical Reviews* does not list an abbreviation or the abbreviation might prove confusing. Volume numbers are in Arabic numerals in keeping with current library custom. We have tried to be accurate in reporting the historical developments and assigning credit; moreover, we

Cambridge University Press

0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Frontmatter/Prelims

[More information](#)

vi

have cited all the works that we have consulted. We apologize in advance for any omissions and slights that perhaps remain.

The book was begun on 11 February 1990; the construction of the “manuscript” and the collaborative effort was almost exclusively electronic, using the EMACS editor in conjunction with \LaTeX and relying on NSFNET to transfer files between us. We have, for this second printing, updated the bibliography and corrected all the typographical errors that have come to our attention since publication, but otherwise the book is essentially the same as the original.

Contents

Preface	v
1 Designs	1
1.1 Introduction	1
1.2 Basic definitions	1
1.3 Related structures	13
1.4 Ranks of incidence matrices	17
1.5 Arcs and ovals	19
1.6 Block's theorem	20
2 Codes	25
2.1 Introduction	25
2.2 Linear codes	31
2.3 Parity-check matrices	35
2.4 Codes from designs	41
2.5 Hamming codes	55
2.6 Cyclic codes	60
2.7 Transforms	66
2.8 Cyclic codes through roots	71
2.9 MDS codes	74
2.10 Quadratic-residue codes	76
2.11 Weight enumerators	81
3 The geometry of vector spaces	89
3.1 Introduction	89
3.2 Projective geometry	90
3.3 Affine geometry	96
3.4 Designs from geometries	99
3.5 The cross ratio	101
3.6 Desargues' theorem	103
3.7 Quadrics and hermitian varieties	104

4	Symmetric Designs	117
4.1	Introduction	117
4.2	The parameters	118
4.3	Automorphisms	122
4.4	Difference sets	123
4.5	Group algebras	129
4.6	The codes and the multiplier theorem	132
5	The standard geometric codes	139
5.1	Introduction	139
5.2	The Reed-Muller codes	140
5.3	Geometries and Reed-Muller codes	145
5.4	Generalized Reed-Muller codes	152
5.5	Dimensions and minimum weights	160
5.6	The geometric codes	167
5.7	The subfield subcodes	177
5.8	Summation formulas for the p -rank	193
6	Codes from planes	199
6.1	Introduction	199
6.2	Projective to affine and back	201
6.3	The codes	203
6.4	The minimum-weight vectors	209
6.5	Central collineations	214
6.6	Other geometric codewords	218
6.7	Hermitian unitals	225
6.8	Translation planes	228
6.9	Tame planes and a rigidity theorem	235
6.10	Derivations	238
6.11	Ovals and derivation sets	243
6.12	Other derivation sets	245
7	Hadamard designs	249
7.1	Introduction	249
7.2	Hadamard designs	251
7.3	Equivalent matrices	255
7.4	The codes	258
7.5	Kronecker product constructions	263
7.6	Size 16 and special n -tuples	266
7.7	Geometric constructions	269
7.8	The Paley construction	271
7.9	Bent functions	275

Cambridge University Press

0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key

Frontmatter/Prelims

[More information](#)

<i>Contents</i>	ix
7.10 Regular Hadamard matrices	278
7.11 Hadamard matrices of size 24	284
7.12 Hadamard matrices from Steiner systems	288
8 Steiner systems	295
8.1 Introduction	295
8.2 Steiner triple and quadruple systems	296
8.3 Unitals	298
8.4 Oval designs	304
8.5 Some Steiner 3-designs	309
8.6 Witt designs and Golay codes	312
Bibliography	317
Glossary	337
Index of Names	339
Index of Terms	344

List of Figures

1.1	The Fano plane	4
1.2	The block $B_{3,2}$ of the biplane	5
1.3	Pascal triangle for designs	8
1.4	Triangle for a 2-design	10
2.1	A noisy communications channel	26
2.2	Hamming code	38
3.1	Harmonic conjugates	101
3.2	Desargues' theorem	103
5.1	The affine plane $AG_2(\mathbf{F}_3)$	164
5.2	The incidence matrix of $AG_2(\mathbf{F}_3)$	165
6.1	Planes of orders 0, 1 and 2	201
8.1	The binary codes of $\mathcal{H}(3)$ and $\mathcal{R}(3)$	302
8.2	Block intersection numbers for the 5-(24, 8, 1) design	315

List of Tables

2.1	The weight distribution for the plane $PG_2(\mathbf{F}_8)$	83
2.2	The complete weight distribution for the plane $PG_2(\mathbf{F}_3)$	85
7.1	Binary codes of the 24×24 Hadamard matrices	286