

Graduate Texts in Mathematics 86

Editorial Board

J.H. Ewing F.W. Gehring P.R. Halmos

Graduate Texts in Mathematics

- 1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
- 2 OXTOBY. Measure and Category. 2nd ed.
- 3 SCHAEFFER. Topological Vector Spaces.
- 4 HILTON/STAMMBACH. A Course in Homological Algebra.
- 5 MAC LANE. Categories for the Working Mathematician.
- 6 HUGHES/PIPER. Projective Planes.
- 7 SERRE. A Course in Arithmetic.
- 8 TAKEUTI/ZARING. Axiomatic Set Theory.
- 9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
- 10 COHEN. A Course in Simple Homotopy Theory.
- 11 CONWAY. Functions of One Complex Variable. 2nd ed.
- 12 BEALS. Advanced Mathematical Analysis.
- 13 ANDERSON/FULLER. Rings and Categories of Modules.
- 14 GOLUBITSKY GUILLEMIN. Stable Mappings and Their Singularities.
- 15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
- 16 WINTER. The Structure of Fields.
- 17 ROSENBLATT. Random Processes. 2nd ed.
- 18 HALMOS. Measure Theory.
- 19 HALMOS. A Hilbert Space Problem Book. 2nd ed., revised.
- 20 HUSEMOLLER. Fibre Bundles. 2nd ed.
- 21 HUMPHREYS. Linear Algebraic Groups.
- 22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
- 23 GREUB. Linear Algebra. 4th ed.
- 24 HOLMES. Geometric Functional Analysis and Its Applications.
- 25 HEWITT/STROMBERG. Real and Abstract Analysis.
- 26 MANES. Algebraic Theories.
- 27 KELLEY. General Topology.
- 28 ZARISKI/SAMUEL. Commutative Algebra. Vol. I.
- 29 ZARISKI/SAMUEL. Commutative Algebra. Vol. II.
- 30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
- 31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
- 32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
- 33 HIRSCH. Differential Topology.
- 34 SPITZER. Principles of Random Walk. 2nd ed.
- 35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
- 36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
- 37 MONK. Mathematical Logic.
- 38 GRAUERT/FRITZSCHE. Several Complex Variables.
- 39 ARVESON. An Invitation to C^* -Algebras.
- 40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
- 41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
- 42 SERRE. Linear Representations of Finite Groups.
- 43 GILLMAN/JERISON. Rings of Continuous Functions.
- 44 KENDIG. Elementary Algebraic Geometry.
- 45 LOËVE. Probability Theory I. 4th ed.
- 46 LOËVE. Probability Theory II. 4th ed.
- 47 MOISE. Geometric Topology in Dimensions 2 and 3.

continued after index

J.H. van Lint

Introduction to Coding Theory

Second Edition



Springer-Verlag

Berlin Heidelberg New York London Paris
Tokyo Hong Kong Barcelona Budapest

J.H. van Lint
Eindhoven University of Technology
Department of Mathematics
Den Dolech 2, P.O. Box 513
5600 MB Eindhoven
The Netherlands

Editorial Board:

J.H. Ewing
Department of
Mathematics
Indiana University
Bloomington, IN 47405
USA

F.W. Gehring
Department of
Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

P.R. Halmos
Department of
Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

Mathematics Subject Classifications (1991): 94-01, 11T71

Library of Congress Cataloging-in-Publication Data

Lint, Jacobus Hendricus van, 1932–
Introduction to coding theory, 2^d ed. / J.H. van Lint.
p. cm.—(Graduate texts in mathematics; 86)
Includes bibliographical references and index.

ISBN 978-3-662-00176-9

1. Coding theory. I. Title. II. Series.

QA268.L57 1992

003'.54—dc20

92-3247

Printed on acid-free paper.

© 1982, 1992 by Springer-Verlag Berlin Heidelberg.

Softcover reprint of the hardcover 2nd edition 1992

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in other ways, and storage in data banks. Duplication of this publication or parts thereof is only permitted under the provisions of the German Copyright Law of September 9, 1965, in its version of June 24, 1985, and a copyright fee must always be paid. Violations fall under the prosecution act of the German Copyright Law. The use of general descriptive names, trade marks, etc. in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Dimitry L. Loseff; manufacturing supervised by Robert Paella.
Typeset by Asco Trade Typesetting Ltd., Hong Kong.

9 8 7 6 5 4 3 2 1

ISBN 978-3-662-00176-9

ISBN 978-3-662-00174-5 (eBook)

DOI 10.1007/978-3-662-00174-5

Preface to the Second Edition

The first edition of this book was conceived in 1981 as an alternative to outdated, oversized, or overly specialized textbooks in this area of discrete mathematics—a field that is still growing in importance as the need for mathematicians and computer scientists in industry continues to grow.

The body of the book consists of two parts: a rigorous, mathematically oriented first course in coding theory followed by introductions to special topics. The second edition has been largely expanded and revised. The main editions in the second edition are:

- (1) a long section on the binary Golay code;
- (2) a section on Kerdock codes;
- (3) a treatment of the Van Lint-Wilson bound for the minimum distance of cyclic codes;
- (4) a section on binary cyclic codes of even length;
- (5) an introduction to algebraic geometry codes.

Eindhoven
November 1991

J.H. VAN LINT

Preface to the First Edition

Coding theory is still a young subject. One can safely say that it was born in 1948. It is not surprising that it has not yet become a fixed topic in the curriculum of most universities. On the other hand, it is obvious that discrete mathematics is rapidly growing in importance. The growing need for mathematicians and computer scientists in industry will lead to an increase in courses offered in the area of discrete mathematics. One of the most suitable and fascinating is, indeed, coding theory. So, it is not surprising that one more book on this subject now appears. However, a little more justification and a little more history of the book are necessary. At a meeting on coding theory in 1979 it was remarked that there was no book available that could be used for an introductory course on coding theory (mainly for mathematicians but also for students in engineering or computer science). The best known textbooks were either too old, too big, too technical, too much for specialists, etc. The final remark was that my Springer Lecture Notes (#201) were slightly obsolete and out of print. Without realizing what I was getting into I announced that the statement was not true and proved this by showing several participants the book *Inleiding in de Coderingstheorie*, a little book based on the syllabus of a course given at the Mathematical Centre in Amsterdam in 1975 (M.C. Syllabus 31). The course, which was a great success, was given by M.R. Best, A.E. Brouwer, P. van Emde Boas, T.M.V. Janssen, H.W. Lenstra Jr., A. Schrijver, H.C.A. van Tilborg and myself. Since then the book has been used for a number of years at the Technological Universities of Delft and Eindhoven.

The comments above explain why it seemed reasonable (to me) to translate the Dutch book into English. In the name of Springer-Verlag I thank the Mathematical Centre in Amsterdam for permission to do so. Of course it turned out to be more than a translation. Much was rewritten or expanded,

problems were changed and solutions were added, and a new chapter and several new proofs were included. Nevertheless the M.C. Syllabus (and the Springer Lecture Notes 201) are the basis of this book.

The book consists of three parts. Chapter 1 contains the prerequisite mathematical knowledge. It is written in the style of a memory-refresher. The reader who discovers topics that he does not know will get some idea about them but it is recommended that he also looks at standard textbooks on those topics. Chapters 2 to 6 provide an introductory course in coding theory. Finally, Chapters 7 to 11 are introductions to special topics and can be used as supplementary reading or as a preparation for studying the literature.

Despite the youth of the subject, which is demonstrated by the fact that the papers mentioned in the references have 1974 as the average publication year, I have not considered it necessary to give credit to every author of the theorems, lemmas, etc. Some have simply become standard knowledge.

It seems appropriate to mention a number of textbooks that I use regularly and that I would like to recommend to the student who would like to learn more than this introduction can offer. First of all F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes* (reference [46]), which contains a much more extensive treatment of most of what is in this book and has 1500 references! For the more technically oriented student with an interest in decoding, complexity questions, etc. E.R. Berlekamp's *Algebraic Coding Theory* (reference [2]) is a must. For a very well-written mixture of information theory and coding theory I recommend: R.J. McEliece, *The Theory of Information and Coding* (reference [51]). In the present book very little attention is paid to the relation between coding theory and combinatorial mathematics. For this the reader should consult P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and their Links* (reference [11]).

I sincerely hope that the time spent writing this book (instead of doing research) will be considered well invested.

Eindhoven
July 1981

J.H. VAN LINT

Second edition comments: Apparently the hope expressed in the final line of the preface of the first edition came true: a second edition has become necessary. Several misprints have been corrected and also some errors. In a few places some extra material has been added.

Contents

Preface to the Second Edition	v
Preface to the First Edition	vii
CHAPTER 1	
Mathematical Background	1
1.1. Algebra	1
1.2. Krawtchouk Polynomials	14
1.3. Combinatorial Theory	17
1.4. Probability Theory	19
CHAPTER 2	
Shannon's Theorem	22
2.1. Introduction	22
2.2. Shannon's Theorem	27
2.3. Comments	29
2.4. Problems	29
CHAPTER 3	
Linear Codes	31
3.1. Block Codes	31
3.2. Linear Codes	33
3.3. Hamming Codes	36
3.4. Majority Logic Decoding	37
3.5. Weight Enumerators	38
3.6. Comments	40
3.7. Problems	40

CHAPTER 4	
Some Good Codes	42
4.1. Hadamard Codes and Generalizations	42
4.2. The Binary Golay Code	43
4.3. The Ternary Golay Code	46
4.4. Constructing Codes from Other Codes	46
4.5. Reed–Muller Codes	48
4.6. Kerdock Codes	54
4.7. Comments	55
4.8. Problems	56
CHAPTER 5	
Bounds on Codes	58
5.1. Introduction: The Gilbert Bound	58
5.2. Upper Bounds	61
5.3. The Linear Programming Bound	68
5.4. Comments	72
5.5. Problems	73
CHAPTER 6	
Cyclic Codes	75
6.1. Definitions	75
6.2. Generator Matrix and Check Polynomial	77
6.3. Zeros of a Cyclic Code	78
6.4. The Idempotent of a Cyclic Code	80
6.5. Other Representations of Cyclic Codes	83
6.6. BCH Codes	85
6.7. Decoding BCH Codes	92
6.8. Reed–Solomon Codes and Algebraic Geometry Codes	93
6.9. Quadratic Residue Codes	96
6.10. Binary Cyclic codes of length $2n$ (n odd)	99
6.11. Comments	100
6.12. Problems	101
CHAPTER 7	
Perfect Codes and Uniformly Packed Codes	102
7.1. Lloyd’s Theorem	102
7.2. The Characteristic Polynomial of a Code	105
7.3. Uniformly Packed Codes	108
7.4. Examples of Uniformly Packed Codes	110
7.5. Nonexistence Theorems	113
7.6. Comments	116
7.7. Problems	117

CHAPTER 8	
Goppa Codes	118
8.1. Motivation	118
8.2. Goppa Codes	119
8.3. The Minimum Distance of Goppa Codes	120
8.4. Asymptotic Behaviour of Goppa Codes	121
8.5. Decoding Goppa Codes	122
8.6. Generalized BCH Codes	123
8.7. Comments	125
8.8. Problems	125
CHAPTER 9	
Asymptotically Good Algebraic Codes	127
9.1. A Simple Nonconstructive Example	127
9.2. Justesen Codes	128
9.3. Comments	132
9.4. Problems	132
CHAPTER 10	
Arithmetic Codes	133
10.1. AN Codes	133
10.2. The Arithmetic and Modular Weight	135
10.3. Mandelbaum–Barrows Codes	139
10.4. Comments	140
10.5. Problems	140
CHAPTER 11	
Convolutional Codes	141
11.1. Introduction	141
11.2. Decoding of Convolutional Codes	145
11.3. An Analog of the Gilbert Bound for Some Convolutional Codes	147
11.4. Construction of Convolutional Codes from Cyclic Block Codes	148
11.5. Automorphisms of Convolutional Codes	151
11.6. Comments	153
11.7. Problems	154
Hints and Solutions to Problems	155
References	174
Index	179