Graduate Texts in Mathematics

J.H. van Lint

Introduction to Coding Theory

Third Edition

编码论导论　第3版

Springer-Verlag
世界图书出版公司

J. H. van Lint

Introduction to Coding Theory

Third Revised and Expanded Edition

Springer

书　　名：Introduction to Coding Theory 3rd ed.
作　　者：J.H.van Lint
中 译 名：编码论导论 第3版
出 版 者：世界图书出版公司北京公司
印 刷 者：北京世图印刷厂
发　　行：世界图书出版公司北京公司 (北京朝内大街137号　100010)
开　　本：24　　印　张：10.5
出版年代：2003年 1月
书　　号：7-5062-0116-X
版权登记：图字:01-2002-5624
定　　价：29.00元

世界图书出版公司北京公司已获得Springer-Verlag授权在中国大陆独家重印发行。

Graduate Texts in Mathematics 86

Editorial Board
S. Axler
F. W. Gehring
K. A. Ribet

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

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. 2nd ed.
5 Mac Lane. Categories for the Working Mathematician. 2nd ed.
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 I. 2nd ed.
12 Beals. Advanced Mathematical Analysis.
13 Anderson/Fuller. Rings and Categories of Modules. 2nd ed.
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 Husemöller. 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 Loève. Probability Theory I. 4th ed.
46 Loève. Probability Theory II. 4th ed.
47 Moise. Geometric Topology in Dimensions 2 and 3.
48 Sachs/Wu. General Relativity for Mathematicians.
49 Gruenberg/Weir. Linear Geometry. 2nd ed.
50 Edwards. Fermat's Last Theorem.
51 Klingenberg. A Course in Differential Geometry.
52 Hartshorne. Algebraic Geometry.
53 Manin. A Course in Mathematical Logic.
54 Graver/Watkins. Combinatorics with Emphasis on the Theory of Graphs.
55 Brown/Pearcy. Introduction to Operator Theory I: Elements of Functional Analysis.
56 Massey. Algebraic Topology: An Introduction
57 Crowell/Fox. Introduction to Knot Theory.
58 Koblitz. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 Lang. Cyclotomic Fields.
60 Arnold. Mathematical Methods in Classical Mechanics. 2nd ed.
61 Whitehead. Elements of Homotopy Theory.
62 Kargapolov/Merzljakov. Fundamentals of the Theory of Groups.
63 Bollobás. Graph Theory.
64 Edwards. Fourier Series. Vol. I. 2nd ed.

continued after index

此为试读,需要完整PDF请访问: www.ertongbook.com

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

S. Axler
Mathematics Department
San Francisco
State University
San Francisco, CA 94132
USA

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

K. A. Ribet
Mathematics Department
University of California
at Berkeley
Berkeley, CA 94720-3840
USA

Library of Congress Cataloging-in-Publication Data

Lint, Jacobus Hendricus van, 1932-
Introduction to coding theory / J.H. van Lint. -- 3rd rev. and expanded ed.
p. cm. -- (Graduate texts in mathematics, 0072-5285 ; 86)
Includes bibliographical references and index.
ISBN 3540641335 (hardcover : alk. paper)
1. Coding theory. I. Title. II. Series.
QA268 .L57 1998
003'.54--dc21

98-48080
CIP

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

ISSN 0072-5285
ISBN 3-540-64133-5 Springer-Verlag Berlin Heidelberg New York
ISBN 3-540-54894-7 2nd Edition Springer-Verlag Berlin Heidelberg New York

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.
Reprinted in China by Beijing World Publishing Corporation, 2003

© Springer-Verlag Berlin Heidelberg 1982, 1992, 1999

Typesetting: Asco Trade Typesetting Ltd., Hong Kong
SPIN 10668931 46/3143 – 5 4 3 2 1 0 – Printed on acid-free paper

Preface to the Third Edition

It is gratifying that this textbook is still sufficiently popular to warrant a third edition. I have used the opportunity to improve and enlarge the book.

When the second edition was prepared, only two pages on algebraic geometry codes were added. These have now been removed and replaced by a relatively long chapter on this subject. Although it is still only an introduction, the chapter requires more mathematical background of the reader than the remainder of this book.

One of the very interesting recent developments concerns binary codes defined by using codes over the alphabet $\mathbb{Z}_4$. There is so much interest in this area that a chapter on the essentials was added. Knowledge of this chapter will allow the reader to study recent literature on $\mathbb{Z}_4$-codes.

Furthermore, some material has been added that appeared in my Springer Lecture Notes **201**, but was not included in earlier editions of this book, e. g. Generalized Reed-Solomon Codes and Generalized Reed-Muller Codes. In Chapter 2, a section on "Coding Gain" (the engineer's justification for using error-correcting codes) was added.

For the author, preparing this third edition was a most welcome return to mathematics after seven years of administration. For valuable discussions on the new material, I thank C. P. J. M. Baggen, I. M. Duursma, H. D. L. Hollmann, H. C. A. van Tilborg, and R. M. Wilson. A special word of thanks to R. A. Pellikaan for his assistance with Chapter 10.

Eindhoven J.H. VAN LINT
November 1998

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 J.H. VAN LINT
November 1991

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 Third Edition V
Preface to the Second Edition VII
Preface to the First Edition IX

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. On Coding Gain 29
2.4. Comments 31
2.5. Problems 32

CHAPTER 3
Linear Codes 33

3.1. Block Codes 33
3.2. Linear Codes 35
3.3. Hamming Codes 38

此为试读,需要完整PDF请访问: www.ertongbook.com

3.4. Majority Logic Decoding 39
3.5. Weight Enumerators 40
3.6. The Lee Metric 42
3.7. Comments 44
3.8. Problems 45

CHAPTER 4
Some Good Codes 47

4.1. Hadamard Codes and Generalizations 47
4.2. The Binary Golay Code 48
4.3. The Ternary Golay Code 51
4.4. Constructing Codes from Other Codes 51
4.5. Reed–Muller Codes 54
4.6. Kerdock Codes 60
4.7. Comments 61
4.8. Problems 62

CHAPTER 5
Bounds on Codes 64

5.1. Introduction: The Gilbert Bound 64
5.2. Upper Bounds 67
5.3. The Linear Programming Bound 74
5.4. Comments 78
5.5. Problems 79

CHAPTER 6
Cyclic Codes 81

6.1. Definitions 81
6.2. Generator Matrix and Check Polynomial 83
6.3. Zeros of a Cyclic Code 84
6.4. The Idempotent of a Cyclic Code 86
6.5. Other Representations of Cyclic Codes 89
6.6. BCH Codes 91
6.7. Decoding BCH Codes 98
6.8. Reed–Solomon Codes 99
6.9. Quadratic Residue Codes 103
6.10. Binary Cyclic Codes of Length $2n(n$ odd) 106
6.11. Generalized Reed–Muller Codes 108
6.12. Comments 110
6.13. Problems 111

CHAPTER 7
Perfect Codes and Uniformly Packed Codes 112

7.1. Lloyd's Theorem 112
7.2. The Characteristic Polynomial of a Code 115

7.3. Uniformly Packed Codes 118
7.4. Examples of Uniformly Packed Codes 120
7.5. Nonexistence Theorems 123
7.6. Comments 127
7.7. Problems 127

CHAPTER 8
Codes over $\mathbb{Z}_4$ 128

8.1. Quaternary Codes 128
8.2. Binary Codes Derived from Codes over $\mathbb{Z}_4$ 129
8.3. Galois Rings over $\mathbb{Z}_4$ 132
8.4. Cyclic Codes over $\mathbb{Z}_4$ 136
8.5. Problems 138

CHAPTER 9
Goppa Codes 139

9.1. Motivation 139
9.2. Goppa Codes 140
9.3. The Minimum Distance of Goppa Codes 142
9.4. Asymptotic Behaviour of Goppa Codes 143
9.5. Decoding Goppa Codes 144
9.6. Generalized BCH Codes 145
9.7. Comments 146
9.8. Problems 147

CHAPTER 10
Algebraic Geometry Codes 148

10.1. Introduction 148
10.2. Algebraic Curves 149
10.3. Divisors 155
10.4. Differentials on a Curve 156
10.5. The Riemann–Roch Theorem 158
10.6. Codes from Algebraic Curves 160
10.7. Some Geometric Codes 162
10.8. Improvement of the Gilbert–Varshamov Bound 165
10.9. Comments 165
10.10.Problems 166

CHAPTER 11
Asymptotically Good Algebraic Codes 167

11.1. A Simple Nonconstructive Example 167
11.2. Justesen Codes 168
11.3. Comments 172
11.4. Problems 172

CHAPTER 12
Arithmetic Codes 173

12.1. AN Codes 173
12.2. The Arithmetic and Modular Weight 175
12.3. Mandelbaum–Barrows Codes 179
12.4. Comments 180
12.5. Problems 180

CHAPTER 13
Convolutional Codes 181

13.1. Introduction 181
13.2. Decoding of Convolutional Codes 185
13.3. An Analog of the Gilbert Bound for Some Convolutional Codes 187
13.4. Construction of Convolutional Codes from Cyclic Block Codes 188
13.5. Automorphisms of Convolutional Codes 191
13.6. Comments 193
13.7. Problems 194

Hints and Solutions to Problems 195

References 218

Index 223

CHAPTER 1

Mathematical Background

In order to be able to read this book a fairly thorough mathematical background is necessary. In different chapters many different areas of mathematics play a rôle. The most important one is certainly algebra but the reader must also know some facts from elementary number theory, probability theory and a number of concepts from combinatorial theory such as designs and geometries. In the following sections we shall give a brief survey of the prerequisite knowledge. Usually proofs will be omitted. For these we refer to standard textbooks. In some of the chapters we need a large number of facts concerning a not too well-known class of orthogonal polynomials, called Krawtchouk polynomials. These properties are treated in Section 1.2. The notations that we use are fairly standard. We mention a few that may not be generally known. If C is a finite set we denote the number of elements of C by $|C|$. If the expression B is the definition of concept A then we write $A := B$. We use "iff" for "if and only if". An identity matrix is denoted by I and the matrix with all entries equal to one is J. Similarly we abbreviate the vector with all coordinates 0 (resp. 1) by $\mathbf{0}$ (resp. $\mathbf{1}$). Instead of using $[x]$ we write $\lfloor x \rfloor := \max\{n \in \mathbb{Z} | n \leq x\}$ and we use the symbol $\lceil x \rceil$ for rounding upwards.

§1.1. Algebra

We need only very little from elementary number theory. We assume known that in $\mathbb{N}$ every number can be written in exactly one way as a product of prime numbers (if we ignore the order of the factors). If a divides b, then we write $a|b$. If p is a prime number and $p^r|a$ but $p^{r+1} \nmid a$, then we write $p^r \| a$. If

$k \in \mathbb{N}$, $k > 1$, then a representation of n in the base k is a representation

$$n = \sum_{i=0}^{l} n_i k^i,$$

$0 \leq n_i < k$ for $0 \leq i \leq l$. The largest integer n such that $n|a$ and $n|b$ is called the greatest common divisor of a and b and denoted by g.c.d.(a, b) or simply (a, b). If $m|(a - b)$ we write $a \equiv b \pmod{m}$.

(1.1.1) Theorem. *If*

$$\varphi(n) := |\{m \in \mathbb{N} \mid 1 \leq m \leq n, (m, n) = 1\}|,$$

then

(i) $\varphi(n) = n \prod_{p|n}(1 - 1/p)$,
(ii) $\sum_{d|n} \varphi(d) = n$.

The function φ is called the *Euler indicator*.

(1.1.2) Theorem. *If* $(a, m) = 1$ *then* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem 1.1.2 is called the Euler–Fermat theorem.

(1.1.3) Definition. The *Möbius function* μ is defined by

$$\mu(n) := \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct prime factors,} \\ 0, & \text{otherwise.} \end{cases}$$

(1.1.4) Theorem. *If* f *and* g *are functions defined on* $\mathbb{N}$ *such that*

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Theorem 1.1.4 is known as the *Möbius inversion formula.*

Algebraic Structures

We assume that the reader is familiar with the basic ideas and theorems of linear algebra although we do refresh his memory below. We shall first give a sequence of definitions of algebraic structures with which the reader must be familiar in order to appreciate algebraic coding theory.

(1.1.5) Definition. A *group* $(G, \ )$ is a set G on which a product operation has been defined satisfying

(i) $\forall_{a\in G}\forall_{b\in G}[ab \in G]$,
(ii) $\forall_{a\in G}\forall_{b\in G}\forall_{c\in G}[(ab)c = a(bc)]$,
(iii) $\exists_{e\in G}\forall_{a\in G}[ae = ea = a]$,
(the element e is unique),
(iv) $\forall_{a\in G}\exists_{b\in G}[ab = ba = e]$,
(b is called the inverse of a and also denoted by a^{-1}).

If furthermore

(v) $\forall_{a\in G}\forall_{b\in G}[ab = ba]$,

then the group is called *abelian* or *commutative.*

If $(G, \ )$ is a group and $H \subset G$ such that $(H, \ )$ is also a group, then $(H, \ )$ is called a subgroup of $(G, \ )$. Usually we write G instead of $(G, \ )$. The number of elements of a finite group is called the *order* of the group. If $(G, \ )$ is a group and $a \in G$, then the smallest positive integer n such that $a^n = e$ (if such an n exists) is called the *order* of a. In this case the elements $e, a, a^2, \ldots, a^{n-1}$ form a so-called *cyclic* subgroup with a as *generator.* If $(G, \ )$ is abelian and $(H, \ )$ is a subgroup then the sets $aH := \{ah | h \in H\}$ are called *cosets* of H. Since two cosets are obviously disjoint or identical, the cosets form a partition of G. An element chosen from a coset is called a *representative* of the coset. It is not difficult to show that the cosets again form a group if we define multiplication of cosets by $(aH)(bH) := abH$. This group is called the *factor group* and indicated by G/H. As a consequence note that if $a \in G$, then the order of a divides the order of G (also if G is not abelian).

A fundamental theorem of group theory states that a finite abelian group is a direct sum of cyclic groups.

(1.1.6) Definition. A set R with two operations, usually called addition and multiplication, denoted by $(R, +, \ )$, is called a *ring* if

(i) $(R, +)$ is an abelian group,
(ii) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[(ab)c = a(bc)]$,
(iii) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[a(b + c) = ab + ac \wedge (a + b)c = ac + bc]$.

The identity element of $(R, +)$ is usually denoted by 0.

If the additional property

(iv) $\forall_{a\in R}\forall_{b\in R}[ab = ba]$

holds, then the ring is called *commutative.*

The integers $\mathbb{Z}$ are the best known example of a ring.

If $(R, +, \ )$ is a commutative ring, a nonzero element $a \in R$ is called a *zero divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$. If a nontrivial

此为试读,需要完整PDF请访问: www.ertongbook.com