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

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

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

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
November 1998

J.H. VAN LINT

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

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*

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

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

ring has no zero divisors, it is called an *integral domain*. In the same way that $\mathbb{Z}$ is extended to $\mathbb{Q}$, an integral domain can be embedded in its *field of fractions* or *quotient field*.

(1.1.7) Definition. If $(R, +,)$ is a ring and $\emptyset \neq S \subseteq R$, then S is called an *ideal* if

(i) $\forall_{a \in S} \forall_{b \in S} [a - b \in S]$,
(ii) $\forall_{a \in S} \forall_{b \in R} [ab \in S \wedge ba \in S]$.

It is clear that if S is an ideal in R, then $(S, +,)$ is a subring, but requirement (ii) says more than that.

(1.1.8) Definition. A *field* is a ring $(R, +,)$ for which $(R \setminus \{0\},)$ is an abelian group.

(1.1.9) Theorem. *Every finite ring R with at least two elements such that*

$$\forall_{a \in R} \forall_{b \in R} [ab = 0 \Rightarrow (a = 0 \vee b = 0)]$$

is a field.

(1.1.10) Definition. Let $(V, +)$ be an abelian group, $\mathbb{F}$ a field and let a multiplication $\mathbb{F} \times V \to V$ be defined satisfying

(i) $\forall_{\mathbf{a} \in V} [1\mathbf{a} = \mathbf{a}]$,
$\forall_{\alpha \in \mathbb{F}} \forall_{\beta \in \mathbb{F}} \forall_{\mathbf{a} \in V} [\alpha(\beta\mathbf{a}) = (\alpha\beta)\mathbf{a}]$,
(ii) $\forall_{\alpha \in \mathbb{F}} \forall_{\mathbf{a} \in V} \forall_{\mathbf{b} \in V} [\alpha(\mathbf{a} + \mathbf{b}) = \alpha\mathbf{a} + \alpha\mathbf{b}]$,
$\forall_{\alpha \in \mathbb{F}} \forall_{\beta \in \mathbb{F}} \forall_{\mathbf{a} \in V} [(\alpha + \beta)\mathbf{a} = \alpha\mathbf{a} + \beta\mathbf{a}]$.

Then the triple $(V, +, \mathbb{F})$ is called a *vector space* over the field $\mathbb{F}$. The identity element of $(V, +)$ is denoted by $\mathbf{0}$.

We assume the reader to be familiar with the vector space $\mathbb{R}^n$ consisting of all n-tuples $(a_1, a_2, \ldots, a_n)$ with the obvious rules for addition and multiplication. We remind him of the fact that a *k-dimensional subspace* C of this vector space is a vector space with a *basis* consisting of vectors $\mathbf{a}_1 := (a_{11}, a_{12}, \ldots, a_{1n})$, $\mathbf{a}_2 := (a_{21}, a_{22}, \ldots, a_{2n})$, $\ldots$, $\mathbf{a}_k := (a_{k1}, a_{k2}, \ldots, a_{kn})$, where the word basis means that every $\mathbf{a} \in C$ can be written in a unique way as $\alpha_1\mathbf{a}_1 + \alpha_2\mathbf{a}_2 + \cdots + \alpha_k\mathbf{a}_k$. The reader should also be familiar with the process of going from one basis of C to another by taking combinations of basis vectors, etc. We shall usually write vectors as *row vectors* as we did above. The *inner product* $\langle \mathbf{a}, \mathbf{b} \rangle$ of two vectors $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$\langle \mathbf{a}, \mathbf{b} \rangle := a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

The elements of a basis are called *linearly independent*. In other words this means that a linear combination of these vectors is $\mathbf{0}$ iff all the coefficients are 0. If $\mathbf{a}_1, \ldots, \mathbf{a}_k$ are k linearly independent vectors, i.e. a basis of a k-dimensional

subspace C, then the system of equations $\langle \mathbf{a}_i, \mathbf{y} \rangle = 0$ $(i = 1, 2, \ldots, k)$ has as its solution all the vectors in a subspace of dimension $n - k$ which we denote by $C^{\perp}$. So,

$$C^{\perp} := \{\mathbf{y} \in \mathbb{R}^n | \forall_{\mathbf{x} \in C}[\langle \mathbf{x}, \mathbf{y} \rangle = 0]\}.$$

These ideas play a fundamental role later on, where $\mathbb{R}$ is replaced by a finite field $\mathbb{F}$. The theory reviewed above goes through in that case.

(1.1.11) Definition. Let $(V, +)$ be a vector space over $\mathbb{F}$ and let a multiplication $V \times V \to V$ be defined that satisfies

(i) $(V, +, \ )$ is a ring,
(ii) $\forall_{\alpha \in \mathbb{F}} \forall_{\mathbf{a} \in V} \forall_{\mathbf{b} \in V}[(\alpha \mathbf{a})\mathbf{b} = \mathbf{a}(\alpha \mathbf{b})]$.

Then we say that the system is an *algebra* over $\mathbb{F}$.

Suppose we have a finite group $(G, \cdot)$ and we consider the elements of G as basis vectors for a vector space $(V, +)$ over a field $\mathbb{F}$. Then the elements of V are represented by linear combinations $\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n$, where

$$\alpha_i \in \mathbb{F}, \qquad g_i \in G, \qquad (1 \leq i \leq n = |G|).$$

We can define a multiplication $*$ for these vectors in the obvious way, namely

$$\left(\sum_i \alpha_i g_i\right) * \left(\sum_j \beta_j g_j\right) := \sum_i \sum_j (\alpha_i \beta_j)(g_i \cdot g_j),$$

which can be written as $\sum_k \gamma_k g_k$, where γ_k is the sum of the elements $\alpha_i \beta_j$ over all pairs (i, j) such that $g_i \cdot g_j = g_k$. This yields an algebra which is called the *group algebra* of G over $\mathbb{F}$ and denoted by $\mathbb{F}G$.

EXAMPLES. Let us consider a number of examples of the concepts defined above.

If $A := \{a_1, a_2, \ldots, a_n\}$ is a finite set, we can consider all one-to-one mappings of S onto S. These are called *permutations*. If σ_1 and σ_2 are permutations we define $\sigma_1 \sigma_2$ by $(\sigma_1 \sigma_2)(a) := \sigma_1(\sigma_2(a))$ for all $a \in A$. It is easy to see that the set S_n of all permutations of A with this multiplication is a group, known as the *symmetric group of degree n*. In this book we shall often be interested in special permutation groups. These are subgroups of S_n. We give one example. Let C be a k-dimensional subspace of $\mathbb{R}^n$. Consider all permutations σ of the integers $1, 2, \ldots, n$ such that for every vector $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$ the vector $(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)})$ is also in C. These clearly form a subgroup of S_n. Of course C will often be such that this subgroup of S consists of the identity only but there are more interesting examples! Another example of a permutation group which will turn up later is the *affine permutation group* defined as follows. Let $\mathbb{F}$ be a (finite) field. The mapping $f_{u,v}$, when $u \in \mathbb{F}$, $v \in \mathbb{F}$, $u \neq 0$, is defined on $\mathbb{F}$ by $f_{u,v}(x) := ux + v$ for all $x \in \mathbb{F}$. These mappings are permutations of $\mathbb{F}$ and clearly they form a group under composition of functions.