

Lecture Notes in Mathematics

A collection of informal reports and seminars

Edited by A. Dold, Heidelberg and B. Eckmann, Zürich

Series: California Institute of Technology, Pasadena

Adviser: C. R. DePrima

201

Jacobus H. van Lint

California Institute of Technology, Pasadena, CA/USA

Coding Theory

Second Printing



Springer-Verlag

Berlin · Heidelberg · New York 1973

AMS Subject Classifications (1970): 94 A 10

ISBN 3-540-06363-3 Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-06363-3 Springer-Verlag New York · Heidelberg · Berlin

ISBN 3-540-05476-6 1. Auflage Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-05476-6 1st edition Springer-Verlag New York · Heidelberg · Berlin

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks.

Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© by Springer-Verlag Berlin · Heidelberg 1973. Library of Congress Catalog Card Number 73-83239. Printed in Germany.

Offsetdruck: Julius Beltz, Hemsbach

PREFACE

These lecture notes are the contents of a two-term course given by me during the 1970-1971 academic year as Morgan Ward visiting professor at the California Institute of Technology. The students who took the course were mathematics seniors and graduate students. Therefore a thorough knowledge of algebra (a.o. linear algebra, theory of finite fields, characters of abelian groups) and also probability theory were assumed. After introducing coding theory and linear codes these notes concern topics mostly from algebraic coding theory. The practical side of the subject, e.g. circuitry, is not included. Some topics which one would like to include in a course for students of mathematics such as bounds on the information rate of codes and many connections between combinatorial mathematics and coding theory could not be treated due to lack of time. For an extension of the course into a third term these two topics would have been chosen.

Although the material for this course came from many sources there are three which contributed heavily and which were used as suggested reading material for the students. These are W. W. Peterson's Error-Correcting Codes ([15]), E. R. Berlekamp's Algebraic Coding Theory ([5]) and several of the AFCRL-reports by E. F. Assmus, H. F. Mattson and R. Turyn ([2], [3], [4] a.o.). For several fruitful discussions I would like to thank R. J. McEliece.

The extensive treatment of perfect codes is due to my own interest in this topic and recent developments. The reader who is familiar with coding theory will notice that in several places I have given a new treatment or new proofs of known theorems. Since coding theory is young there remain several parts which need polishing and several problems are still open. I sincerely hope that the course and these notes will contribute to the growing interest of mathematicians in this fascinating subject.

For her excellent typing of these lecture notes I thank Mrs. L. Decker.

Pasadena, March 1971.

J. H. van Lint.

CONTENTS

CHAPTER I: Introduction

1.1	Channels, noise, redundancy	1
1.2	An introductory example.....	4
1.3	Some definitions in information theory	8
1.4	Shannon's fundamental theorem.....	10
1.5	Problems.....	13

CHAPTER II: Linear codes

2.1	General theory.....	15
2.2	Hamming codes.....	20
2.3	Reed-Muller codes	27
2.4	Threshold decoding	32
2.5	Direct-product codes.....	36
2.6	Problems.....	40

CHAPTER III: Cyclic codes

3.1	Introduction	42
3.2	The zeros of a cyclic code	46
3.3	Idempotents	49
3.4	Some other representations of cyclic codes	55
3.5	Problems.....	59

VI

CHAPTER IV: Important cyclic codes

4.1	BCH codes	61
4.2	Reed-Solomon codes	70
4.3	Generalized Reed-Muller codes	75
4.4	Quadratic residue codes	79
4.5	Problems	85

CHAPTER V: Perfect codes

5.1	Perfect single-error-correcting codes.....	86
5.2	The sphere-packing condition.....	92
5.3	The Golay codes	98
5.4	Lloyd's theorem	104
5.5	Nonexistence theorems	112

CHAPTER VI: Weight enumeration

6.1	The MacWilliams equations	120
6.2	Weight enumeration of Reed-Muller codes	122
6.3	The Carlitz-Uchiyama bound	127
	References	130
	Index	132

NOTATION

$P(a)$ and $\text{Prob}(a)$ denote the probability of the event a .

Vectors are denoted by underlined symbols, e.g. \underline{x} , \underline{y} , $\underline{\theta}$.

$(\underline{a}, \underline{b})$ is the usual inner product.

$\underline{a} \cdot \underline{b}$ is a product of vectors which is defined in (2.3.1).

$\mathbb{R}^{(n)}$ is the n -dimensional vector space (over a specified field $\text{GF}(q)$).

Systems with binary operations are denoted by giving the set and the operation, e.g. $(\text{GF}(q)[x], +, \cdot)$ is the ring of polynomials with coefficients in $\text{GF}(q)$ and addition denoted by $+$ and multiplication denoted without a special symbol.

For matrices A and vectors \underline{x} the transpose is A^T resp. \underline{x}^T .

If a and b are integers then $a|b$ means " a divides b ".

If p is a prime then $p^e || n$ means " $p^e | n$ and $p^{e+1} \nmid n$ ".

$A := B$ is used when the expression B defines A .

$A \subset B$ does not exclude $A = B$.

[] refers to the references at the end of the notes.