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

Springer-Verlag Berlin Heidelberg GmbH 1971

AMS Subject Classifications (1970): 94 A 10

ISBN 978-3-540-05476-4 **ISBN 978-3-662-20712-3 (eBook)**
DOI 10.1007/978-3-662-20712-3

Originally published by Springer-Verlag Berlin . Heidelberg · New York in 1971

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 IV: Important cyclic codes

CHAPTER V: Perfect codes

CHAPTER VI: Weight enumeration

NOTATION

P(a) and 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.

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

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

Systems with binary operations are denoted by giving the set and the operation, e.g. $(GF(q)[x],+,\ )$ is the ring of polynomials with coefficients in 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.