

Elements of Algebraic Coding Theory

CHAPMAN & HALL MATHEMATICS SERIES

Editors:

Professor Keith Devlin
St Mary's College
USA

Professor Derek Goldrei
Open University
UK

Dr James Montaldi
Université de Lille
France

OTHER TITLES IN THE SERIES INCLUDE

Dynamical Systems
Differential equations, maps and
chaotic behaviour
D. K. Arrowsmith and C. M. Place

Network Optimization
V. K. Balakrishnan

Algebraic Numbers and Algebraic
Functions
P. M. Cohn

Elements of Linear Algebra
P. M. Cohn

Control and Optimization
B. D. Craven

Sets, Functions and Logic
A foundation course in mathematics
Second edition
K. Devlin

Functions of Two Variables
S. Dineen

The Dynamic Cosmos
M. S. Madsen

Full information on the complete range of Chapman & Hall mathematics books is available from the publishers.

JOIN US ON THE INTERNET VIA WWW, GOPHER, FTP OR EMAIL:

WWW: <http://www.thomson.com>

GOPHER: <gopher.thomson.com>

FTP: <ftp.thomson.com>

EMAIL: findit@kiosk.thomson.com

A service of **I(T)P**

Elements of Algebraic Coding Theory

L. R. Vermani

Professor of Mathematics
Kurukshetra University
Kurukshetra, India



Springer-Science+Business Media, B.V.

First edition 1996

© 1996 L. R. Vermani

Originally published by Chapman & Hall in 1996

Typeset in 10/12 pt Times by Thomson Press (India) Ltd, New Delhi, India

ISBN 978-0-412-57380-4

ISBN 978-1-4899-7268-2 (eBook)

DOI 10.1007/978-1-4899-7268-2

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the UK Copyright Designs and Patents Act, 1988, this publication may not be reproduced, stored or transmitted, in any form or by any means, without the prior permission in writing of the publishers, or in the case of reprographic reproduction only in accordance with the terms of the licences issued by the Copyright Licensing Agency in the UK, or in accordance with the terms of licences issued by the appropriate Reproduction Rights Organization outside the UK. Enquiries concerning reproduction outside the terms stated here should be sent to the publishers at the London address printed on this page.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

A catalogue record for this book is available from the British Library

Library of Congress Catalog Card Number: 96-84046



Printed on permanent acid-free text paper, manufactured in accordance with ANSI/NISO Z39.48-1992 and ANSI/NISO Z39.48-1984 (Permanence of Paper).

Contents

Preface	vii
1 Group codes	1
1.1 Elementary properties	1
1.2 Matrix encoding techniques	8
1.3 Generator and parity check matrices	14
2 Polynomial codes	24
2.1 Definition of vector space and polynomial ring	24
2.2 Polynomial codes	26
2.3 Generator and parity check matrices – general case	34
3 Hamming codes	39
3.1 Binary representation of numbers	39
3.2 Hamming codes	41
4 Finite fields and BCH codes	47
4.1 Finite fields	47
4.2 Some examples of primitive polynomials	62
4.3 Bose–Chaudhuri–Hocquenghem codes	65
5 Linear codes	81
5.1 Generator and parity check matrices	81
5.2 Dual code of a linear code	87
5.3 Weight distribution of the dual code of a binary linear code	97
5.4 New codes obtained from given codes	102
6 Cyclic codes	107
6.1 Cyclic codes	107
6.2 Check polynomial	111

6.3	BCH and Hamming codes as cyclic codes	114
6.4	Non-binary Hamming codes	119
6.5	Idempotents	129
6.6	Some solved examples and an invariance property	131
6.7	Cyclic codes and group algebras	135
6.8	Self dual binary cyclic codes	137
7	Factorization of polynomials	140
7.1	Factors of $X^n - 1$	140
7.2	Factorization through cyclotomic cosets	143
7.3	Berlekamp's algorithm for factorization of polynomials	149
7.4	Berlekamp's algorithm – a special case	157
8	Quadratic residue codes	172
8.1	Introduction	172
8.2	Some examples of quadratic residue codes	176
8.3	Extended quadratic residue codes and distance properties	180
8.4	Idempotents of quadratic residue codes	194
8.5	Some examples	202
9	Maximum distance separable codes	208
9.1	Necessary and sufficient conditions for MDS codes	208
9.2	The weight distribution of MDS codes	215
9.3	An existence problem	218
9.4	Reed–Solomon codes	220
10	Automorphism group of a code	223
10.1	Automorphism group of a binary code	223
10.2	Automorphism group of a non-binary code	229
10.3	Automorphism group – its relation with minimum distance	234
11	Hadamard matrices and Hadamard codes	242
11.1	Hadamard matrices	242
11.2	Hadamard codes	248
Bibliography		251
Index		253

Preface

Coding theory came into existence in connection with some engineering problems in the late 1940s (1948–50 to be precise). The subject developed by using sophisticated mathematical techniques including algebraic. The aspect of the subject using algebraic techniques came to be known as Algebraic Coding Theory. The subject is concerned with devising ‘efficient’ encoding and decoding procedures. There are by now about half a dozen books written on the subject besides a couple of books on Applied Modern Algebra containing some aspects of the subject. The present book is mainly based on a course of lectures given at Kurukshetra University to mathematics students during the last few years. For giving this course of lectures, the books by MacWilliams and Sloane (1978), Van Lint (1971), Birkhoff and Bartee (1970), Dornhoff and Hohn (1978) were used extensively. The object of the present book is to present only the fundamentals of the subject keeping a first-year student in view. However, an effort is made to give a rigorous treatment with full details (even though sometimes trivial and except for some results from Algebra which are accepted without proofs) and the material covered may be regarded as a first course on the subject.

We start with the definition of a block code and of distance between words of equal length. Using the maximum likelihood decoding procedure, we obtain necessary and sufficient conditions for a code to (i) detect, (ii) correct any set of k or fewer errors. Two very important and useful algebraic methods of defining codes (encoding procedures) are through matrix and polynomial multiplication. The codes obtained are called respectively matrix codes and polynomial codes. These two types of codes are studied in Chapters 1 and 2. Generator and parity check matrices are also discussed here.

Hamming codes are single error correcting codes which are studied using a constructive approach in Chapter 3. For defining Hamming codes, we need the binary representation of numbers which is discussed in the first section of this chapter.

One of the most important classes of codes invented so far is that of Bose–Chaudhuri–Hocquenghem (BCH) codes. These are polynomial codes and are

discussed in Chapter 4. For defining BCH codes, we need quite a few results from finite fields. Construction of finite fields is of paramount importance for these codes and is discussed at length although some results needed from rings are assumed. Some BCH codes of smaller lengths are constructed.

Linear codes are subspaces of finite dimensional vector spaces over a finite field and are discussed in Chapter 5. The concept of dual code is introduced and MacWilliams's identity relating the weight enumerator of the dual of a binary linear code with that of the code is given.

Cyclic codes can be identified as ideals in a certain quotient ring of a polynomial ring and are discussed in Chapter 6. Among other results, it is proved that BCH codes and Hamming codes are cyclic codes. Non-binary Hamming codes are defined and it is proved that Hamming codes (binary as well as non-binary) are perfect codes. A couple of examples of binary cyclic self dual codes are given. Study of cyclic codes raises the problem of factorization of the polynomial $X^m - 1$ as a product of irreducible polynomials and is discussed in Chapter 7. Berlekamp's Algorithm (1968) regarding factorization of any polynomial over a finite field is also discussed. A number of examples illustrating the algorithm are given—in particular factorization of the binary polynomial $X^{61} - 1$ is obtained.

In Chapter 8, we study quadratic residue (QR) codes. Binary Golay code \mathcal{G}_{23} and ternary Golay code \mathcal{G}_{11} occur as examples of quadratic residue codes. Certain minimum distance properties of QR codes and the relationship between extended QR codes and duals of QR codes are obtained. Idempotents of binary and ternary QR codes are explicitly given.

Maximum distance separable (MDS) codes are discussed in Chapter 9 giving among others a necessary and sufficient condition for a linear code to be MDS. The problem of existence of largest possible n for which there is an $[n, k, d]$ MDS code over $\text{GF}(q)$ for a given value of k and q is also considered.

Automorphism group of a code is useful in giving information about the minimum distance of the code. Automorphism group of a code is defined and some simple properties of these are obtained in Chapter 10. It is proved that in a binary cyclic code which is invariant under a certain group of permutations, the weights of all the code words cannot be divisible by 4.

All the codes studied in Chapters 1–10 are group/linear codes. To avoid the impression that perhaps all codes are 'linear', we introduce Hadamard matrices and then define Hadamard codes which are non-linear.

*To my wife Raj
and
daughters Vandana & Shalini*

1

Group codes

1.1 ELEMENTARY PROPERTIES

Definition 1.1 – groups

A non-empty set G with a binary composition is called a **group** if the following hold.

- (i) The composition in G is associative, i.e. $(ab)c = a(bc) \forall a, b, c \in G$.
- (ii) There exists an element $e \in G$ such that $ea = ae = a \forall a \in G$.
- (iii) For every $a \in G$, there exists an element $b \in G$ such that $ab = ba = e$.

It is fairly easy to prove that element $e \in G$ satisfying condition (ii) above is uniquely determined and, then, is called the **identity** of G . Also for $a \in G$, element $b \in G$ satisfying $ab = ba = e$ is uniquely determined and is called the **inverse** of a , denoted by a^{-1} .

Definition 1.2 – Abelian groups

A group G is called **Abelian** if $ab = ba \forall a, b \in G$.

Definition 1.3 – rings

A non-empty set R with two binary compositions, say addition and multiplication, defined on it is called a **ring** if:

- (i) R is an Abelian group w.r.t. the additive composition;
- (ii) multiplication in R is associative, i.e. $(ab)c = a(bc) \forall a, b, c \in R$; and
- (iii) the two distributive laws hold, i.e. $\forall a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

A ring R which also has the property

$$ab = ba \forall a, b \in R$$

is called a **commutative ring**. If R is a ring having an element $1 \in R$ such that $1a = a = a1$ for every $a \in R$, then R is called a **ring with identity**.