

Elements of Algebraic Coding Theory

L. R. Vermani

Professor of Mathematics
Kurukshetra University
Kurukshetra, India



CHAPMAN & HALL

London · Weinheim · New York · Tokyo · Melbourne · Madras

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