

NORTH-HOLLAND
MATHEMATICAL LIBRARY

The Theory of Error- Correcting Codes

F.J. MACWILLIAMS
N.J.A. SLOANE

North-Holland

Contents

Preface	v
Preface to the third printing	xi
Contents	xiii

Chapter 1. Linear codes

1. Linear codes	1
2. Properties of a linear code	5
3. At the receiving end	7
4. More about decoding a linear code	15
5. Error probability	18
6. Shannon's theorem on the existence of good codes	22
7. Hamming codes	23
8. The dual code	26
9. Construction of new codes from old (II)	27
10. Some general properties of a linear code	32
11. Summary of Chapter 1	34
Notes on Chapter 1	34

Chapter 2. Nonlinear codes, Hadamard matrices, designs and the Golay code

1. Nonlinear codes	38
2. The Plotkin bound	41
3. Hadamard matrices and Hadamard codes	44

4. Conference matrices	55
5. t -designs	58
6. An introduction to the binary Golay code	64
7. The Steiner system $S(5, 6, 12)$, and nonlinear single-error correcting codes	70
8. An introduction to the Nordstrom–Robinson code	73
9. Construction of new codes from old (III)	76
Notes on Chapter 2	78

Chapter 3. An introduction to BCH codes and finite fields

1. Double-error-correcting BCH codes (I)	80
2. Construction of the field $GF(16)$	82
3. Double-error-correcting BCH codes (II)	86
4. Computing in a finite field	88
Notes on Chapter 3	92

Chapter 4. Finite fields

1. Introduction	93
2. Finite fields: the basic theory	95
3. Minimal polynomials	99
4. How to find irreducible polynomials	107
5. Tables of small fields	109
6. The automorphism group of $GF(p^m)$	112
7. The number of irreducible polynomials	114
8. Bases of $GF(p^m)$ over $GF(p)$	115
9. Linearized polynomials and normal bases	118
Notes on Chapter 4	124

Chapter 5. Dual codes and their weight distribution

1. Introduction	125
2. Weight distribution of the dual of a binary linear code	125
3. The group algebra	132
4. Characters	134
5. MacWilliams theorem for nonlinear codes	135
6. Generalized MacWilliams theorems for linear codes	141
7. Properties of Krawtchouk polynomials	150
Notes on Chapter 5	153

Chapter 5. Codes, designs and perfect codes

1. Introduction	155
2. Four fundamental parameters of a code	156
3. An explicit formula for the weight and distance distribution	158
4. Designs from codes when $s \leq d'$	160
5. The dual code also gives designs	164
6. Weight distribution of translates of a code	166
7. Designs from nonlinear codes when $s' < d$	174
8. Perfect codes	175
9. Codes over $\text{GF}(q)$	176
10. There are no more perfect codes	179
Notes on Chapter 6	186

Chapter 7. Cyclic codes

1. Introduction	188
2. Definition of a cyclic code	188
3. Generator polynomial	190
4. The check polynomial	194
5. Factors of $x^n - 1$	196
6. t -error-correcting BCH codes	201
7. Using a matrix over $\text{GF}(q^n)$ to define a code over $\text{GF}(q)$	207
8. Encoding cyclic codes	209
Notes on Chapter 7	214

Chapter 8. Cyclic codes (contd.): Idempotents and Mattson-Solomon polynomials

1. Introduction	216
2. Idempotents	217
3. Minimal ideals, irreducible codes, and primitive idempotents	219
4. Weight distribution of minimal codes	227
5. The automorphism group of a code	229
6. The Mattson-Solomon polynomial	239
7. Some weight distributions	251
Notes on Chapter 8	255

Chapter 9. BCH codes

1. Introduction	257
2. The true minimum distance of a BCH code	259

3. The number of information symbols in BCH codes	262
4. A table of BCH codes	266
5. Long BCH codes are bad	269
6. Decoding BCH codes	270
7. Quadratic equations over $GF(2^m)$	277
8. Double-error-correcting BCH codes are quasi-perfect	279
9. The Carlitz–Uchiyama bound	280
10. Some weight distributions are asymptotically normal	282
Notes on Chapter 9	291

Chapter 10. Reed–Solomon and Justesen codes

1. Introduction	294
2. Reed–Solomon codes	294
3. Extended RS codes	296
4. Idempotents of RS codes	296
5. Mapping $GF(2^m)$ codes into binary codes	298
6. Burst error correction	301
7. Encoding Reed–Solomon codes	301
8. Generalized Reed–Solomon codes	303
9. Redundant residue codes	305
10. Decoding RS codes	306
11. Justesen codes and concatenated codes	306
Notes on Chapter 10	315

Chapter 11. MDS codes

1. Introduction	317
2. Generator and parity check matrices	318
3. The weight distribution of an MDS code	319
4. Matrices with every square submatrix nonsingular	321
5. MDS codes from RS codes	323
6. n -arcs	326
7. The known results	327
8. Orthogonal arrays	328
Notes on Chapter 11	329

Chapter 12. Alternant, Goppa and other generalized BCH codes

1. Introduction	332
2. Alternant codes	333

3. Goppa codes	338
4. Further properties of Goppa codes	346
5. Extended double-error-correcting Goppa codes are cyclic	350
6. Generalized Srivastava codes	357
7. Chien-Choy generalized BCH codes	360
8. The Euclidean algorithm	362
9. Decoding alternant codes	365
Notes on Chapter 12	368

Chapter 13. Reed-Muller codes

1. Introduction	370
2. Boolean functions	370
3. Reed-Muller Codes	373
4. RM codes and geometries	377
5. The minimum weight vectors generate the code	381
6. Encoding and decoding (I)	385
7. Encoding and decoding (II)	388
8. Other geometrical codes	397
9. Automorphism groups of the RM codes	398
10. Mattson-Solomon polynomials of RM codes	401
11. The action of the general affine group on Mattson-Solomon polynomials	402
Notes on Chapter 13	403

Chapter 14. First-order Reed-Muller codes

1. Introduction	406
2. Pseudo-noise sequences	406
3. Cosets of the first-order Reed-Muller code	412
4. Encoding and decoding $\mathcal{R}(1, m)$	419
5. Bent functions	426
Notes on Chapter 14	431

Chapter 15. Second-order Reed-Muller, Kerdock and Preparata codes

1. Introduction	433
2. Weight distribution of second-order Reed-Muller codes	434
3. Weight distribution of arbitrary Reed-Muller codes	445
4. Subcodes of dimension $2m$ of $\mathcal{R}(2, m)^*$ and $\mathcal{R}(2, m)$	448
5. The Kerdock code and generalizations	453
6. The Preparata code	466
7. Goethals' generalization of the Preparata codes	476
Notes on Chapter 15	477

Chapter 16. Quadratic-residue codes

1. Introduction	480
2. Definition of quadratic-residue codes	481
3. Idempotents of quadratic-residue codes	484
4. Extended quadratic-residue codes	488
5. The automorphism group of QR codes	491
6. Binary quadratic residue codes	494
7. Double circulant and quasi-cyclic codes	505
8. Quadratic-residue and symmetry codes over GF(3)	510
9. Decoding of cyclic codes and others	512
Notes on Chapter 16	518

Chapter 17. Bounds on the size of a code

1. Introduction	523
2. Bounds on $A(n, d, w)$	524
3. Bounds on $A(n, d)$	531
4. Linear programming bounds	535
5. The Griesmer bound	546
6. Constructing linear codes; anticode	547
7. Asymptotic bounds	556
Notes on Chapter 17	566

Chapter 18. Methods for combining codes

1. Introduction	567
Part I: Product codes and generalizations	
2. Direct product codes	568
3. Not all cyclic codes are direct products of cyclic codes	571
4. Another way of factoring irreducible cyclic codes	573
5. Concatenated codes: the * construction	575
6. A general decomposition for cyclic codes	578
Part II: Other methods of combining codes	
7. Methods which increase the length	581
7.1 Construction X: adding tails to the codewords	581
7.2 Construction X4: combining four codes	584
7.3 Single- and double-error-correcting codes	586

7.4 The $ a+x b+x a+b+x $ construction	587
7.5 Piret's construction	588
8. Constructions related to concatenated codes	589
8.1 A method for improving concatenated codes	589
8.2 Zinov'ev's generalized concatenated codes	590
9. Methods for shortening a code	592
9.1 Constructions Y1-Y4	592
9.2 A construction of Helgert and Stinaff	593
Notes on Chapter 18	594

Chapter 19. Self-dual codes and invariant theory

1. Introduction	596
2. An introduction to invariant theory	598
3. The basic theorems of invariant theory	607
4. Generalizations of Gleason's theorems	617
5. The nonexistence of certain very good codes	624
6. Good self-dual codes exist	629
Notes on Chapter 19	633

Chapter 20. The Golay codes

1. Introduction	634
2. The Mathieu group M_{24}	636
3. M_{24} is five-fold transitive	637
4. The order of M_{24} is 24.23.22.21.20.48	638
5. The Steiner system $S(5, 8, 24)$ is unique	641
6. The Golay codes $\mathcal{G}_{23}$ and $\mathcal{G}_{24}$ are unique	646
7. The automorphism groups of the ternary Golay codes	647
8. The Golay codes $\mathcal{G}_{11}$ and $\mathcal{G}_{12}$ are unique	648
Notes on Chapter 20	649

Chapter 21. Association schemes

1. Introduction	651
2. Association schemes	651
3. The Hamming association scheme	656
4. Metric schemes	659
5. Symplectic forms	661
6. The Johnson scheme	665

7. Subsets of association schemes	666
8. Subsets of symplectic forms	667
9. t -designs and orthogonal arrays	670
Notes on Chapter 21	671

Appendix A. Tables of the best codes known

1. Introduction	673
2. Figure 1, a small table of $A(n, d)$	683
3. Figure 2, an extended table of the best codes known	690
4. Figure 3, a table of $A(n, d, w)$	691

Appendix B. Finite geometries

1. Introduction	692
2. Finite geometries, $PG(m, q)$ and $EG(m, q)$	692
3. Properties of $PG(m, q)$ and $EG(m, q)$	697
4. Projective and affine planes	701
Notes on Appendix B	702

Bibliography	703
Index	757