

Fundamentals of Error-Correcting Codes

W. Cary Huffman

Loyola University of Chicago

and

Vera Pless

University of Illinois at Chicago



Contents

Preface

page xiii

1	Basic concepts of linear codes	1
1.1	Three fields	2
1.2	Linear codes, generator and parity check matrices	3
1.3	Dual codes	5
1.4	Weights and distances	7
1.5	New codes from old	13
1.5.1	Puncturing codes	13
1.5.2	Extending codes	14
1.5.3	Shortening codes	16
1.5.4	Direct sums	18
1.5.5	The $(\mathbf{u} \mid \mathbf{u} + \mathbf{v})$ construction	18
1.6	Permutation equivalent codes	19
1.7	More general equivalence of codes	23
1.8	Hamming codes	29
1.9	The Golay codes	31
1.9.1	The binary Golay codes	31
1.9.2	The ternary Golay codes	32
1.10	Reed–Muller codes	33
1.11	Encoding, decoding, and Shannon’s Theorem	36
1.11.1	Encoding	37
1.11.2	Decoding and Shannon’s Theorem	39
1.12	Sphere Packing Bound, covering radius, and perfect codes	48
2	Bounds on the size of codes	53
2.1	$A_q(n, d)$ and $B_q(n, d)$	53
2.2	The Plotkin Upper Bound	58

2.3	The Johnson Upper Bounds	60
2.3.1	The Restricted Johnson Bound	61
2.3.2	The Unrestricted Johnson Bound	63
2.3.3	The Johnson Bound for $A_q(n, d)$	65
2.3.4	The Nordstrom–Robinson code	68
2.3.5	Nearly perfect binary codes	69
2.4	The Singleton Upper Bound and MDS codes	71
2.5	The Elias Upper Bound	72
2.6	The Linear Programming Upper Bound	75
2.7	The Griesmer Upper Bound	80
2.8	The Gilbert Lower Bound	86
2.9	The Varshamov Lower Bound	87
2.10	Asymptotic bounds	88
2.10.1	Asymptotic Singleton Bound	89
2.10.2	Asymptotic Plotkin Bound	89
2.10.3	Asymptotic Hamming Bound	90
2.10.4	Asymptotic Elias Bound	92
2.10.5	The MRRW Bounds	93
2.10.6	Asymptotic Gilbert–Varshamov Bound	94
2.11	Lexicodes	95

3 Finite fields 100

3.1	Introduction	100
3.2	Polynomials and the Euclidean Algorithm	101
3.3	Primitive elements	104
3.4	Constructing finite fields	106
3.5	Subfields	110
3.6	Field automorphisms	111
3.7	Cyclotomic cosets and minimal polynomials	112
3.8	Trace and subfield subcodes	116

4 Cyclic codes 121

4.1	Factoring $x^n - 1$	122
4.2	Basic theory of cyclic codes	124
4.3	Idempotents and multipliers	132
4.4	Zeros of a cyclic code	141
4.5	Minimum distance of cyclic codes	151
4.6	Meggitt decoding of cyclic codes	158
4.7	Affine-invariant codes	162

5	BCH and Reed–Solomon codes	168
5.1	BCH codes	168
5.2	Reed–Solomon codes	173
5.3	Generalized Reed–Solomon codes	175
5.4	Decoding BCH codes	178
5.4.1	The Peterson–Gorenstein–Zierler Decoding Algorithm	179
5.4.2	The Berlekamp–Massey Decoding Algorithm	186
5.4.3	The Sugiyama Decoding Algorithm	190
5.4.4	The Sudan–Guruswami Decoding Algorithm	195
5.5	Burst errors, concatenated codes, and interleaving	200
5.6	Coding for the compact disc	203
5.6.1	Encoding	204
5.6.2	Decoding	207
6	Duadic codes	209
6.1	Definition and basic properties	209
6.2	A bit of number theory	217
6.3	Existence of duadic codes	220
6.4	Orthogonality of duadic codes	222
6.5	Weights in duadic codes	229
6.6	Quadratic residue codes	237
6.6.1	QR codes over fields of characteristic 2	238
6.6.2	QR codes over fields of characteristic 3	241
6.6.3	Extending QR codes	245
6.6.4	Automorphisms of extended QR codes	248
7	Weight distributions	252
7.1	The MacWilliams equations	252
7.2	Equivalent formulations	255
7.3	A uniqueness result	259
7.4	MDS codes	262
7.5	Coset weight distributions	265
7.6	Weight distributions of punctured and shortened codes	271
7.7	Other weight enumerators	273
7.8	Constraints on weights	275
7.9	Weight preserving transformations	279
7.10	Generalized Hamming weights	282

8	Designs	291
8.1	t -designs	291
8.2	Intersection numbers	295
8.3	Complementary, derived, and residual designs	298
8.4	The Assmus–Mattson Theorem	303
8.5	Codes from symmetric 2-designs	308
8.6	Projective planes	315
8.7	Cyclic projective planes	321
8.8	The nonexistence of a projective plane of order 10	329
8.9	Hadamard matrices and designs	330
9	Self-dual codes	338
9.1	The Gleason–Pierce–Ward Theorem	338
9.2	Gleason polynomials	340
9.3	Upper bounds	344
9.4	The Balance Principle and the shadow	351
9.5	Counting self-orthogonal codes	359
9.6	Mass formulas	365
9.7	Classification	366
	9.7.1 The Classification Algorithm	366
	9.7.2 Gluing theory	370
9.8	Circulant constructions	376
9.9	Formally self-dual codes	378
9.10	Additive codes over \mathbb{F}_4	383
9.11	Proof of the Gleason–Pierce–Ward Theorem	389
9.12	Proofs of some counting formulas	393
10	Some favorite self-dual codes	397
10.1	The binary Golay codes	397
	10.1.1 Uniqueness of the binary Golay codes	397
	10.1.2 Properties of binary Golay codes	401
10.2	Permutation decoding	402
10.3	The hexacode	405
	10.3.1 Uniqueness of the hexacode	405
	10.3.2 Properties of the hexacode	406
	10.3.3 Decoding the Golay code with the hexacode	407
10.4	The ternary Golay codes	413

10.4.1	Uniqueness of the ternary Golay codes	413
10.4.2	Properties of ternary Golay codes	418
10.5	Symmetry codes	420
10.6	Lattices and self-dual codes	422

11 Covering radius and cosets 432

11.1	Basics	432
11.2	The Norse Bound and Reed–Muller codes	435
11.3	Covering radius of BCH codes	439
11.4	Covering radius of self-dual codes	444
11.5	The length function	447
11.6	Covering radius of subcodes	454
11.7	Ancestors, descendants, and orphans	459

12 Codes over \mathbb{Z}_4 467

12.1	Basic theory of \mathbb{Z}_4 -linear codes	467
12.2	Binary codes from \mathbb{Z}_4 -linear codes	472
12.3	Cyclic codes over \mathbb{Z}_4	475
12.3.1	Factoring $x^n - 1$ over \mathbb{Z}_4	475
12.3.2	The ring $\mathfrak{R}_n = \mathbb{Z}_4[x]/(x^n - 1)$	480
12.3.3	Generating polynomials of cyclic codes over \mathbb{Z}_4	482
12.3.4	Generating idempotents of cyclic codes over \mathbb{Z}_4	485
12.4	Quadratic residue codes over \mathbb{Z}_4	488
12.4.1	\mathbb{Z}_4 -quadratic residue codes: $p \equiv -1 \pmod{8}$	490
12.4.2	\mathbb{Z}_4 -quadratic residue codes: $p \equiv 1 \pmod{8}$	492
12.4.3	Extending \mathbb{Z}_4 -quadratic residue codes	492
12.5	Self-dual codes over \mathbb{Z}_4	495
12.5.1	Mass formulas	498
12.5.2	Self-dual cyclic codes	502
12.5.3	Lattices from self-dual codes over \mathbb{Z}_4	503
12.6	Galois rings	505
12.7	Kerdock codes	509
12.8	Preparata codes	515

13 Codes from algebraic geometry 517

13.1	Affine space, projective space, and homogenization	517
13.2	Some classical codes	520

13.2.1	Generalized Reed–Solomon codes revisited	520
13.2.2	Classical Goppa codes	521
13.2.3	Generalized Reed–Solomon codes	524
13.3	Algebraic curves	526
13.4	Algebraic geometry codes	532
13.5	The Gilbert–Varshamov Bound revisited	541
13.5.1	Goppa codes meet the Gilbert–Varshamov Bound	541
13.5.2	Algebraic geometry codes exceed the Gilbert–Varshamov Bound	543

14 **Convolutional codes** 546

14.1	Generator matrices and encoding	546
14.2	Viterbi decoding	551
14.2.1	State diagrams	551
14.2.2	Trellis diagrams	554
14.2.3	The Viterbi Algorithm	555
14.3	Canonical generator matrices	558
14.4	Free distance	562
14.5	Catastrophic encoders	568

15 **Soft decision and iterative decoding** 573

15.1	Additive white Gaussian noise	573
15.2	A Soft Decision Viterbi Algorithm	580
15.3	The General Viterbi Algorithm	584
15.4	Two-way APP decoding	587
15.5	Message passing decoding	593
15.6	Low density parity check codes	598
15.7	Turbo codes	602
15.8	Turbo decoding	607
15.9	Some space history	611

	<i>References</i>	615
	<i>Symbol index</i>	630
	<i>Subject index</i>	633