

# Contents

<b>Preface</b>	<b>xi</b>
<b>Introduction</b>	<b>xiii</b>
<b>1 Fundamentals</b>	<b>1</b>
1.1 Weight, distance	3
1.1.1 Minimum distance, and error correction	4
1.1.2 Hamming bound	6
1.2 Parity check matrix and syndrome	7
1.3 Decoding principles	8
1.4 Error probability	11
1.5 Hamming codes	13
1.6 Generator matrix	15
1.7 Code, encoding and and equivalent codes	16
1.8 Cyclic codes	16
1.9 Dual codes	17
1.10 Shortening and extension of codes	17
1.11 Channel capacity and the coding theorem	19
1.12 Summary	21
1.13 Problems	22
<b>2 Galois fields</b>	<b>25</b>
2.1 Groups	25
2.2 Rings, fields	26
2.3 Prime fields	27
2.3.1 Primitive elements	28

2.3.2	Euclidean algorithm	29
2.3.3	Gaussian integers	32
2.4	Extension fields	34
2.4.1	Irreducible polynomials	34
2.4.2	Primitive polynomials and roots of polynomials	36
2.4.3	Properties of extension fields	38
2.5	Cyclotomic cosets	40
2.6	Quadratic residues	41
2.7	Summary	42
2.8	Problems	42
<b>3</b>	<b>Reed–Solomon codes</b>	<b>45</b>
3.1	Definition of RS codes	45
3.1.1	Discrete Fourier transform (DFT)	47
3.1.2	Generator polynomial	48
3.1.3	Parity check polynomial	49
3.1.4	Encoding	50
3.1.5	General definition of RS codes	51
3.1.6	Generalized RS codes and extended RS codes	51
3.2	Algebraic decoding	55
3.2.1	Key equation	57
3.2.2	Berlekamp–Massey algorithm	62
3.2.3	Euclidean algorithm	63
3.2.4	Calculation of the error values	70
3.2.5	Equivalence of the Euclidean and Berlekamp–Massey algorithms	73
3.2.6	Erasure correction	74
3.3	Summary	76
3.4	Problems	77
<b>4</b>	<b>BCH codes</b>	<b>81</b>
4.1	Primitive BCH codes	81
4.1.1	Definition based on cyclotomic cosets	81
4.1.2	Designed distance	83
4.1.3	Definition by the DFT	84
4.1.4	Properties of primitive BCH codes	85
4.1.5	Calculation of the generator polynomial	86
4.2	Non-primitive BCH codes	88
4.3	Shortening and extending BCH codes	89
4.4	Non-binary BCH codes	89
4.5	Relationship between BCH and RS codes	90
4.6	Asymptotic behavior of BCH codes	90
4.7	Decoding of BCH codes	91
4.8	Summary	92
4.9	Problems	93

<b>5</b>	<b>Other classes of codes</b>	<b>95</b>
5.1	First-order Reed–Muller codes, simplex codes and Walsh sequences	95
5.1.1	Reed–Muller and Hamming codes	97
5.1.2	Hamming and simplex codes	98
5.1.3	Simplex codes and binary pseudonoise (PN) sequences	99
5.1.4	Reed–Muller and simplex codes	102
5.2	Reed–Muller codes of higher order	104
5.3	$q$ -ary Hamming codes	107
5.4	Quadratic residue codes	109
5.5	Consta- and negacyclic codes	110
5.6	Binary interpretation of codes over $GF(q = 2^m)$ and $\mathbb{Z}_4$	112
5.7	Summary	113
5.8	Problems	114
<b>6</b>	<b>The trellis representation and properties of block codes</b>	<b>117</b>
6.1	Cyclic dual codes	117
6.2	MacWilliams identity	120
6.3	Automorphism	122
6.4	Gilbert–Varshamov bound	123
6.5	Singleton bound (MDS)	124
6.6	Reiger bound (burst error correction)	125
6.7	Asymptotic bounds	126
6.8	Minimal trellis of linear block codes	127
6.8.1	Construction with the aid of the parity check matrix	129
6.8.2	Construction with the aid of the generator matrix	131
6.8.3	Properties of a minimal trellis	136
6.9	Summary	140
6.10	Problems	142
<b>7</b>	<b>Decoding of block codes</b>	<b>143</b>
7.1	Channel models and metrics	144
7.1.1	$q$ -ary symmetric channel	145
7.1.2	Additive white Gaussian noise (AWGN)	146
7.1.3	Time-variant channels	147
7.1.4	Hamming and Euclidean metrics	149
7.2	Decoder principles, reliability, complexity and coding gain	150
7.2.1	Decoding principles	150
7.2.2	Reliability and decoding principles for binary transmission	151
7.2.3	Decoding complexity and Evseev’s lemma	157
7.2.4	Coding gain	158
7.3	Decoding methods without reliability information	160
7.3.1	Permutation decoding	160
7.3.2	Majority logic decoding	163
7.3.3	DA algorithm	165
7.3.4	Hard-decision maximum-likelihood decoding: Viterbi algorithm	168
7.4	Decoding methods using reliability information	170
7.4.1	Symbolwise soft-decision decoding	170

7.4.2	List decoding using code trellises: Viterbi algorithm	177
7.4.3	List decoding in the code space $\mathcal{C}$	180
7.4.4	List decoding based on ordered statistics	189
7.4.5	List decoding in code space $\mathcal{C}^\perp$	192
7.5	Decoding as an optimization problem	195
7.6	Summary	198
7.7	Problems	199
<b>8</b>	<b>Convolutional codes</b>	<b>201</b>
8.1	Fundamentals of convolutional codes	202
8.1.1	Encoding with sequential logic	202
8.1.2	Impulse response and convolution	204
8.1.3	Constraint length, memory and overall constraint length	206
8.1.4	Generator matrix in the time domain	207
8.1.5	State diagram, code tree and trellis	210
8.1.6	Free distance and path enumerators	213
8.1.7	Termination, truncation and tail-biting	217
8.1.8	Generator matrix in the $Z$ domain	220
8.1.9	Systematic and catastrophic generator matrices	224
8.1.10	Punctured convolutional codes	226
8.2	Algebraic description	230
8.2.1	Code, generator matrix and encoder	230
8.2.2	Convolutional encoder in controller and observer canonical form	230
8.2.3	Equivalent generator matrices	233
8.2.4	Generator matrix in Smith form	235
8.2.5	Basic generator matrix	237
8.2.6	Catastrophic generator matrices	239
8.2.7	Systematic generator matrices	240
8.2.8	Parity check matrix and dual code	242
8.3	Distance measures	244
8.3.1	Row and column distance	244
8.3.2	Extended distance measures	247
8.4	Maximum-likelihood (Viterbi) decoding	251
8.4.1	Metrics	252
8.4.2	Viterbi algorithm	254
8.4.3	Bounds for decoding performance	257
8.4.4	Interleaving	260
8.4.5	Soft-output Viterbi algorithm (SOVA)	261
8.5	Maximum a posteriori decoding (MAP)	264
8.5.1	BCJR algorithm	264
8.5.2	Max log MAP algorithm	267
8.6	Sequential decoding	268
8.6.1	Fano metric	269
8.6.2	Zigangirov–Jelinek (ZJ) decoder	271
8.6.3	Fano decoder	271
8.7	(Partial) unit memory codes, (P)UM codes	272
8.7.1	Definition of (P)UM codes	273

8.7.2	Trellis of (P)UM codes	275
8.7.3	Distance measures for (P)UM codes	276
8.7.4	Construction of (P)UM codes	277
8.7.5	BMD decoding	279
8.8	Tables of good codes	281
8.9	Summary	285
8.10	Problems	286
<b>9</b>	<b>Generalized code concatenation</b>	<b>287</b>
9.1	Introductory examples	290
9.2	GC codes with block codes	295
9.2.1	Definition of GC codes	296
9.2.2	Partitioning of block codes	298
9.2.3	Code construction	305
9.2.4	Decoding of GC codes	312
9.2.5	Unequal error protection (UEP) codes	328
9.2.6	Cyclic codes as GC codes	329
9.2.7	Error locating codes	334
9.2.8	Error locating codes in two dimensions	340
9.3	GC codes with convolutional codes	344
9.3.1	Partitioning of (P)UM codes	345
9.3.2	Introductory example of trellis partitioning	349
9.3.3	Partitioning of convolutional codes	356
9.3.4	Construction and decoding of a GC code	361
9.4	GC codes with block and convolutional codes	367
9.4.1	Inner convolutional and outer block codes	367
9.4.2	Inner block and outer convolutional codes	371
9.5	Multiple concatenation and Reed–Muller codes	373
9.5.1	GMC decoding algorithm for RM codes	375
9.5.2	L-GMC, list decoding of RM codes	380
9.5.3	Simulation results and computational complexity	383
9.6	Summary	387
<b>10</b>	<b>Coded modulation</b>	<b>391</b>
10.1	Introductory examples	392
10.2	GC with block modulation	393
10.2.1	Partitioning of signals	394
10.2.2	Definition of coded modulation	396
10.2.3	Lattices and generalized multilevel concatenation	398
10.2.4	Decoding	402
10.2.5	Trellis-coded modulation systems	405
10.3	GC with convolutional modulation	407
10.3.1	Introductory example	408
10.3.2	Algebraic description of convolutional modulation	409
10.3.3	Partitioning of convolutional modulation	412
10.3.4	Outer convolutional codes	413
10.3.5	Outer block codes	416

10.4 Summary	417
<b>A Serial and parallel concatenated codes and their iterative decoding: turbo codes</b>	<b>419</b>
A.1 Serial code concatenation	420
A.2 Parallel code concatenation	424
A.3 Iterative decoding	428
A.4 Properties and performance aspects of serial and parallel concatenated codes	431
<b>B Metrics</b>	<b>437</b>
B.1 Lee metric	438
B.2 Manhattan and Mannheim metrics	440
B.3 Combinational metrics	441
<b>C Log likelihood algebra</b>	<b>445</b>
<b>D Solutions</b>	<b>447</b>
References	475
Index	489