
Contents

Preface	xiii
List of Acronyms	xv
Notations	xix
Introduction	xxiii
Chapter 1. Introduction to Information Theory	1
1.1. Introduction	1
1.2. Review of probabilities	2
1.2.1. Discrete random variables	2
1.2.2. Continuous random variables	4
1.2.3. Jensen's inequality	5
1.2.4. Random signals	5
1.3. Entropy and mutual information	7
1.3.1. Comments on the concept of information	7
1.3.2. A logarithmic measure of information	7
1.3.3. Mutual information	10
1.3.4. Entropy and average mutual information	11
1.3.5. Kullback–Leibler divergence	15
1.3.6. Differential entropy	15
1.3.7. Typical and jointly typical sequences	17
1.4. Lossless source coding theorems	20
1.4.1. Introduction	20

1.4.2. Entropy and source redundancy	20
1.4.3. Fundamental theorem of source coding	22
1.4.4. Lossless source coding	23
1.5. Theorem for lossy source coding	30
1.5.1. Introduction	30
1.5.2. Definitions	30
1.5.3. Lossy source coding theorem	31
1.6. Transmission channel models	34
1.6.1. Binary symmetric channel	34
1.6.2. Discrete channels without memory	36
1.6.3. Binary erasure channel	38
1.6.4. Additive white Gaussian noise channel	38
1.7. Capacity of a transmission channel	40
1.7.1. Introduction	40
1.7.2. Capacity of a transmission channel	40
1.7.3. Fundamental theorem of channel coding	42
1.7.4. Capacity of the binary symmetric channel	43
1.7.5. Capacity of erasure channel	45
1.7.6. Capacity of additive white Gaussian noise channel	46
1.7.7. Graphical representation	49
1.8. Exercises	54
1.8.1. Exercise 1: calculation of the entropy for a discrete channel	54
1.8.2. Exercise 2: computation of the mutual information	55
1.8.3. Exercise 3: capacity of the additive white Gaussian noise channel	55
1.8.4. Exercise 4: binary symmetric channel	55
1.8.5. Exercise 5: Z channel	56
1.8.6. Exercise 6: discrete channel	56
Chapter 2. Source Coding	57
2.1. Introduction	57
2.2. Algorithms for lossless source coding	58
2.2.1. Run length coding	58
2.2.2. Huffman's algorithm	58
2.2.3. Evaluation of the entropy of a written text	60
2.2.4. Arithmetic coding	63

2.2.5. Algorithm LZ78	65
2.2.6. Lempel–Ziv–Welch (LZW) algorithm	67
2.3. Sampling and quantization	69
2.3.1. Review of the sampling theorem	69
2.3.2. Scalar quantization	70
2.3.3. Optimal scalar quantization	78
2.3.4. Vector quantization	81
2.3.5. Optimal vector quantization	86
2.4. Coding techniques for analog sources with memory	87
2.4.1. Introduction	87
2.4.2. Linear prediction	88
2.4.3. Predictive scalar quantization	91
2.4.4. Transform coding	96
2.4.5. Subband coding	99
2.5. Application to the image and sound compression	101
2.5.1. Application to the still image compression	101
2.5.2. Application to speech coding	102
2.5.3. Application to audio compression	109
2.6. Exercises	116
2.6.1. Exercise 1: entropy and Huffman’s coding	116
2.6.2. Exercise 2: entropy and Huffman’s coding for a source with memory	116
2.6.3. Exercise 3: LZ78 encoding and decoding	116
2.6.4. Exercise 4: scalar quantization and Huffman’s coding	117
2.6.5. Exercise 5: scalar quantization and distortion	117
2.6.6. Exercise 6: DPCM coding and decoding	118
Chapter 3. Linear Block Codes	121
3.1. Introduction	121
3.2. Finite fields	122
3.2.1. Fields	122
3.2.2. Finite fields	123
3.2.3. Irreducible and primitive polynomials	123
3.2.4. Finite field with 2^m elements	125
3.3. Linear block codes	127
3.3.1. Introduction	127
3.3.2. Minimum distance of a code	130

3.3.3. Parity check matrix	131
3.3.4. Weight enumerator functions	132
3.3.5. Error correction and error detection capabilities of linear block codes	134
3.3.6. Bounds on the minimum distance of the linear block codes	136
3.3.7. Bounds on the rate in the non-asymptotic regime	138
3.3.8. Main block codes	142
3.3.9. Graphical representations of binary linear block codes	146
3.4. Decoding of binary linear block codes	152
3.4.1. Introduction	152
3.4.2. Optimal decoding	154
3.4.3. Hard input decoding of binary linear block codes	157
3.4.4. Soft input decoding of binary linear block codes	163
3.4.5. Erasure decoding of binary linear block codes	166
3.5. Performances of linear block codes	172
3.5.1. Performances of linear block codes with hard input decoding	172
3.5.2. Union bound	173
3.5.3. Performances of linear block codes with soft input decoding	175
3.5.4. Coding gain	179
3.5.5. Performance comparison of hard and soft input decoders	182
3.6. Cyclic codes	182
3.6.1. Definition and properties	182
3.6.2. Properties of the cyclic codes	185
3.6.3. Error detection using CRC and automatic repeat request	189
3.6.4. Encoding of cyclic codes	192
3.6.5. Decoding of cyclic codes	198
3.6.6. BCH codes	202
3.6.7. Reed–Solomon codes	213
3.7. Applications	214
3.8. Exercises	216
3.8.1. Exercise 1: repetition code	216

3.8.2. Exercise 2: error probability on a binary symmetric channel	217
3.8.3. Exercise 3: re-emission strategy	217
3.8.4. Exercise 4: simplex code (7,3)	218
3.8.5. Exercise 5: linear block code (6,3)	218
3.8.6. Exercise 6: Hamming code (7,4)	219
3.8.7. Exercise 7: Reed–Muller code (8,4)	219
3.8.8. Exercise 8: hard trellis based decoding of block code	220
3.8.9. Exercise 9: soft trellis based decoding of block code	221
3.8.10. Exercise 10: soft input decoding	222
3.8.11. Exercise 11: comparison of hard and soft decoding	223
3.8.12. Exercise 12: Hamming code	224
3.8.13. Exercise 13: cyclic code	224
3.8.14. Exercise 14: Hamming code	225
3.8.15. Exercise 15: performance of Reed–Solomon code (255,291)	226
3.8.16. Exercise 16: CRC	226
3.8.17. Exercise 17: Reed–Solomon code	227
Chapter 4. Convolutional Codes	229
4.1. Introduction	229
4.2. Mathematical representations and hardware structures	229
4.2.1. Definitions	229
4.2.2. Matrix representation of convolutional codes	235
4.3. Graphical representation of the convolutional codes	238
4.3.1. State transition diagram	238
4.3.2. Trellis diagram	239
4.3.3. TWL graphs	241
4.4. Free distance and transfer function of convolutional codes	242
4.5. Viterbi’s algorithm for the decoding of convolutional codes	246
4.5.1. Complexity of the Viterbi decoder	248
4.6. Punctured convolutional codes	249
4.7. Applications	249

4.8. Exercises	250
4.8.1. Exercise 1: systematic recursive convolutional code	250
4.8.2. Exercise 2: non-recursive code and Viterbi decoding	251

Chapter 5. Concatenated Codes and Iterative Decoding

Chapter 5. Concatenated Codes and Iterative Decoding	253
5.1. Introduction	253
5.2. Soft input soft output decoding	254
5.2.1. Introduction	254
5.2.2. Sum-product algorithm	260
5.2.3. Forward-backward algorithm	269
5.3. LDPC codes	288
5.3.1. Definition	288
5.3.2. LDPC encoding	293
5.3.3. Iterative decoding of the LDPC codes	295
5.3.4. Applications	306
5.4. Parallel concatenated convolutional codes or turbo codes	306
5.4.1. Introduction	306
5.4.2. Structure of the encoder	307
5.4.3. Performance study of turbo codes	311
5.4.4. Iterative decoding of turbo codes	315
5.4.5. EXIT charts	319
5.4.6. Criteria and interleaver design	323
5.4.7. Applications	328
5.5. Other classes of concatenated codes	330
5.5.1. Parallel concatenated block codes	330
5.5.2. Serial concatenated convolutional codes	333
5.5.3. Repeat-accumulate codes	333
5.5.4. Product codes	333
5.6. Exercises	335
5.6.1. Exercise 1: soft input soft output decoding of a two-state convolutional code	335
5.6.2. Exercise 2: soft input soft output decoding of a (4,3) linear block code	336

Appendices	339
Appendix A	341
Appendix B	343
Bibliography	345
Index	353
Summary of Volume 2	355