

Table of Contents

Homage to Alain Glavieux	xv
Chapter 1. Information Theory.	1
G�rard BATTAIL	
1.1. Introduction: the Shannon paradigm	1
1.2. Principal coding functions	5
1.2.1. Source coding	5
1.2.2. Channel coding	6
1.2.3. Cryptography	7
1.2.4. Standardization of the Shannon diagram blocks.	8
1.2.5. Fundamental theorems.	9
1.3. Quantitative measurement of information	9
1.3.1. Principle	9
1.3.2. Measurement of self-information	10
1.3.3. Entropy of a source.	11
1.3.4. Mutual information measure	12
1.3.5. Channel capacity	14
1.3.6. Comments on the measurement of information	15
1.4. Source coding	15
1.4.1. Introduction	15
1.4.2. Decodability, Kraft-McMillan inequality.	16
1.4.3. Demonstration of the fundamental theorem	17
1.4.4. Outline of optimal algorithms of source coding	18
1.5. Channel coding	19
1.5.1. Introduction and statement of the fundamental theorem	19
1.5.2. General comments	20
1.5.3. Need for redundancy	20
1.5.4. Example of the binary symmetric channel	21
1.5.4.1. Hamming’s metric	21
1.5.4.2. Decoding with minimal Hamming distance	22

1.5.4.3. Random coding	23
1.5.4.4. Gilbert-Varshamov bound.	24
1.5.5. A geometrical interpretation	25
1.5.6. Fundamental theorem: Gallager's proof	26
1.5.6.1. Upper bound of the probability of error.	27
1.5.6.2. Use of random coding	28
1.5.6.3. Form of exponential limits	30
1.6. Channels with continuous noise.	32
1.6.1. Introduction	32
1.6.2. A reference model in physical reality: the channel with Gaussian additive noise	32
1.6.3. Communication via a channel with additive white Gaussian noise.	35
1.6.3.1. Use of a finite alphabet, modulation.	35
1.6.3.2. Demodulation, decision margin	36
1.6.4. Channel with fadings.	37
1.7. Information theory and channel coding	38
1.8. Bibliography	40
Chapter 2. Block Codes.	41
Alain POLI	
2.1. Unstructured codes	41
2.1.1. The fundamental question of message redundancy	41
2.1.2. Unstructured codes	42
2.1.2.1. Code parameters	42
2.1.2.2. Code, coding and decoding	43
2.1.2.3. Bounds of code parameters	44
2.2. Linear codes	44
2.2.1. Introduction	44
2.2.2. Properties of linear codes	44
2.2.2.1. Minimum distance and minimum weight of a code.	45
2.2.2.2. Linear code base, coding	45
2.2.2.3. Singleton bound.	46
2.2.3. Dual code	46
2.2.3.1. Reminders of the Gaussian method	46
2.2.3.2. Lateral classes of a linear code C	47
2.2.3.3. Syndromes	48
2.2.3.4. Decoding and syndromes	49
2.2.3.5. Lateral classes, syndromes and decoding.	49
2.2.3.6. Parity check matrix and minimum code weight	49
2.2.3.7. Minimum distance of C and matrix H.	50
2.2.4. Some linear codes	50
2.2.5. Decoding of linear codes	51

2.3. Finite fields	53
2.3.1. Basic concepts.	53
2.3.2. Polynomial modulo calculations: quotient ring	53
2.3.3. Irreducible polynomial modulo calculations: finite field.	54
2.3.4. Order and the opposite of an element of $F_2[X]/(p(X))$	54
2.3.4.1. Order	55
2.3.4.2. Properties of the order	55
2.3.4.3. Primitive elements	56
2.3.4.4. Use of the primitives	58
2.3.4.5. How to find a primitive	58
2.3.4.6. Exponentiation	59
2.3.5. Minimum polynomials.	59
2.3.6. The field of n^{th} roots of unity	60
2.3.7. Projective geometry in a finite field	61
2.3.7.1. Points	61
2.3.7.2. Projective subspaces of order 1.	61
2.3.7.3. Projective subspaces of order t	61
2.3.7.4. An example	61
2.3.7.5. Cyclic codes and projective geometry.	62
2.4. Cyclic codes	62
2.4.1. Introduction	62
2.4.2. Base, coding, dual code and code annihilator	63
2.4.2.1. Cyclic code base	63
2.4.2.2. Coding	64
2.4.2.3. Annihilator and dual of a cyclic code C	65
2.4.2.4. Cyclic code and error correcting capability: roots of $g(X)$	66
2.4.2.5. The Vandermonde determinant.	66
2.4.2.6. BCH theorem	67
2.4.3. Certain cyclic codes	68
2.4.3.1. Hamming codes.	68
2.4.3.2. BCH codes.	69
2.4.3.3. Fire codes	70
2.4.3.4. RM codes	71
2.4.3.5. RS codes	71
2.4.3.6. Codes with true distance greater than their BCH distance	71
2.4.3.7. PG-codes.	71
2.4.3.8. QR codes.	73
2.4.4. Existence and construction of cyclic codes.	74
2.4.4.1. Existence.	74
2.4.4.2. Construction	75
2.4.4.3. Shortened codes and extended codes	79
2.4.4.4. Specifications	79
2.4.4.5. How should we look for a cyclic code?	79
2.4.4.6. How should we look for a truncated cyclic code?	81

2.4.5. Applications of cyclic codes	82
2.5. Electronic circuits	82
2.5.1. Basic gates for error correcting codes	82
2.5.2. Shift registers	83
2.5.3. Circuits for the correct codes	83
2.5.3.1. Divisors.	83
2.5.3.2. Multipliers	84
2.5.3.3. Multiplier-divisors	84
2.5.3.4. Encoder (systematic coding)	84
2.5.3.5. Inverse calculation in F_q	85
2.5.3.6. Hsiao decoder	85
2.5.3.7. Meggitt decoder (natural code).	86
2.5.3.8. Meggitt decoder (shortened code)	87
2.5.4. Polynomial representation and representation to the power of a primitive representation for a field	87
2.6. Decoding of cyclic codes.	88
2.6.1. Meggitt decoding (trapping of bursts).	88
2.6.1.1. The principle of trapping of bursts.	88
2.6.1.2. Trapping in the case of natural Fire codes	88
2.6.1.3. Trapping in the case of shortened Fire codes.	89
2.6.2. Decoding by the DFT	89
2.6.2.1. Definition of the DFT	89
2.6.2.2. Some properties of the DFT.	89
2.6.2.3. Decoding using the DFT.	92
2.6.3. FG-decoding.	94
2.6.3.1. Introduction	94
2.6.3.2. Solving a system of polynomial equations with several variables	95
2.6.3.3. Two basic operations.	96
2.6.3.4. The algorithm of B. Buchberger	96
2.6.3.5. FG-decoding.	97
2.6.4. Berlekamp-Massey decoding	99
2.6.4.1. Introduction	99
2.6.4.2. Existence of a key equation	100
2.6.4.3. The solution by successive stages	100
2.6.4.4. Some properties of d_j	101
2.6.4.5. Property of an optimal solution $(a_j(X), b_j(X))$ at level j	101
2.6.4.6. Construction of the pair $(a'_{j+1}(X), b'_{j+1}(X))$ at the j stage	102
2.6.4.7. Construction of an optimal solution $(a_{j+1}(X), b_{j+1}(X))$	103
2.6.4.8. The algorithm	104
2.6.5. Majority decoding	105
2.6.5.1. The mechanism of decoding, and the associated code	105
2.6.5.2. Trapping by words of $C^\perp$ incidents between them	106

2.6.5.3. Codes decodable in one or two stages	106
2.6.5.4. How should the digital implementation be prepared?	108
2.6.6. Hard decoding, soft decoding and chase decoding	110
2.6.6.1. Hard decoding and soft decoding	110
2.6.6.2. Chase decoding	110
2.7. 2D codes	111
2.7.1. Introduction	111
2.7.2. Product codes	112
2.7.3. Minimum distance of 2D codes	112
2.7.4. Practical examples of the use of 2D codes	112
2.7.5. Coding	112
2.7.6. Decoding	113
2.8. Exercises on block codes	113
2.8.1. Unstructured codes	113
2.8.2. Linear codes	114
2.8.3. Finite bodies	117
2.8.4. Cyclic codes	119
2.8.4.1. Theory	119
2.8.4.2. Applications	122
2.8.5. Exercises on circuits	123
Chapter 3. Convolutional Codes	129
Alain GLAVIEUX and Sandrine VATON	
3.1. Introduction	129
3.2. State transition diagram, trellis, tree	135
3.3. Transfer function and distance spectrum	137
3.4. Perforated convolutional codes	140
3.5. Catastrophic codes	142
3.6. The decoding of convolutional codes	142
3.6.1. Viterbi algorithm	143
3.6.1.1. The term $\log p(S_0)$	144
3.6.1.2. The term $\log p(S_k S_{k-1})$	145
3.6.1.3. The term $\log p(y_k S_k, S_{k-1})$	145
3.6.1.4. Viterbi algorithm	150
3.6.1.5. Viterbi algorithm for transmissions with continuous data flow	155
3.6.2. MAP criterion or BCJR algorithm	156
3.6.2.1. BCJR algorithm	157
3.6.2.2. Example	166
3.6.3. SubMAP algorithm	169
3.6.3.1. Propagation of the Front filter	170
3.6.3.2. Propagation of the Back filter	171
3.6.3.3. Calculation of the $\psi_k(s, s')$ quantities	171
3.6.3.4. Calculation of the joint probability of d_k and y	171

3.7. Performance of convolutional codes	172
3.7.1. Channel with binary input and continuous output	173
3.7.1.1. Gaussian channel	174
3.7.1.2. Rayleigh channel	177
3.7.2. Channel with binary input and output	180
3.8. Distance spectrum of convolutional codes	182
3.9. Recursive convolution codes	184
Chapter 4. Coded Modulations	197
Ezio BIGLIERI	
4.1. Hamming distance and Euclidean distance	197
4.2. Trellis code	200
4.3. Decoding	201
4.4. Some examples of TCM	201
4.5. Choice of a TCM diagram	205
4.6. TCM representations	207
4.7. TCM transparent to rotations	209
4.7.1. Partitions transparent to rotations	211
4.7.2. Transparent trellis with rotations	212
4.7.3. Transparent encoder	213
4.7.4. General considerations	215
4.8. TCM error probability	215
4.8.1. Upper limit of the probability of an error event	215
4.8.1.1. Enumeration of error events	217
4.8.1.2. Interpretation and symmetry	221
4.8.1.3. Asymptotic considerations	223
4.8.1.4. A tighter upper bound	223
4.8.1.5. Bit error probability	224
4.8.1.6. Lower bound of the probability of error	225
4.8.2. Examples	226
4.8.3. Calculation of δ_{free}	228
4.9. Power spectral density	232
4.10. Multi-level coding	234
4.10.1. Block coded modulation	235
4.10.2. Decoding of multilevel codes by stages	237
4.11. Probability of error for the BCM	238
4.11.1. Additive Gaussian channel	239
4.11.2. Calculation of the transfer function	240
4.12. Coded modulations for channels with fading	241
4.12.1. Modeling of channels with fading	241
4.12.1.1. Delay spread	242
4.12.1.2. Doppler-frequency spread	244

4.12.1.3. Classification of channels with fading	244
4.12.1.4. Examples of radio channels with fading	245
4.12.2. Rayleigh fading channel: Euclidean distance and Hamming distance	247
4.13. Bit interleaved coded modulation (BICM).	251
4.14. Bibliography	253
Chapter 5. Turbocodes	255
Claude BERROU, Catherine DOUILLARD, Michel JÉZÉQUEL and Annie PICART	
5.1. History of turbocodes	255
5.1.1. Concatenation	256
5.1.2. Negative feedback in the decoder	256
5.1.3. Recursive systematic codes	258
5.1.4. Extrinsic information.	258
5.1.5. Parallel concatenation	259
5.1.6. Irregular interleaving.	260
5.2. A simple and convincing illustration of the turbo effect	260
5.3. Turbocodes	265
5.3.1. Coding	265
5.3.2. The termination of constituent codes	272
5.3.2.1. Recursive convolutional circular codes	273
5.3.3. Decoding	275
5.3.4. SISO decoding and extrinsic information.	280
5.3.4.1. Notations	280
5.3.4.2. Decoding using the MAP criterion.	281
5.3.4.3. The simplified Max-Log-MAP algorithm	284
5.4. The permutation function.	287
5.4.1. The regular permutation	288
5.4.2. Statistical approach.	290
5.4.3. Real permutations.	291
5.5. m -binary turbocodes.	297
5.5.1. m -binary RSC encoders	298
5.5.2. m -binary turbocodes	300
5.5.3. Double-binary turbocodes with 8 states.	302
5.5.4. Double-binary turbocodes with 16 states	303
5.6. Bibliography	304

Chapter 6. Block Turbocodes	307
Ramesh PYNDIAH and Patrick ADDE	
6.1. Introduction.	307
6.2. Concatenation of block codes	308
6.2.1. Parallel concatenation of block codes	309
6.2.2. Serial concatenation of block codes	313
6.2.3. Properties of product codes and theoretical performances	318
6.3. Soft decoding of block codes	323
6.3.1. Soft decoding of block codes	324
6.3.2. Soft decoding of block codes (Chase algorithm)	326
6.3.3. Decoding of block codes by the Viterbi algorithm	334
6.3.4. Decoding of block codes by the Hartmann and Rudolph algorithm	338
6.4. Iterative decoding of product codes	340
6.4.1. SISO decoding of a block code.	341
6.4.2. Implementation of the weighting algorithm	345
6.4.3. Iterative decoding of product codes	347
6.4.4. Comparison of the performances of BTC.	349
6.5. Conclusion	367
6.6. Bibliography	367
Chapter 7. Block Turbocodes in a Practical Setting	373
Patrick ADDE and Ramesh PYNDIAH	
7.1. Introduction.	373
7.2. Implementation of BTC: structure and complexity	373
7.2.1. Influence of integration constraints	373
7.2.1.1. Quantification of data	373
7.2.1.2. Choice of the scaling factor	375
7.2.2. General architecture and organization of the circuit	376
7.2.2.1. Modular structure.	376
7.2.2.2. Von Neumann architecture	378
7.2.3. Memorizing of data and results.	380
7.2.3.1. Modular structure.	380
7.2.3.2. Von Neumann architecture	381
7.2.4. Elementary decoder	384
7.2.4.1. Decoding of BCH codes with soft inputs and outputs	384
7.2.4.2. Functional structure and sequencing.	385
7.2.4.3. Installation of a decoder on a silicon microchip	388
7.2.5. High flow structure.	392
7.2.5.1. Introduction	392
7.2.5.2. High flow turbodecoder in a practical setting	395
7.3. Flexibility of turbo block codes	397

7.4. Hybrid turbocodes	404
7.4.1. Construction of the code	404
7.4.2. Binary error rates (BER) function of the signal-to-noise ratio in a Gaussian channel	406
7.4.3. Variation of the size of the blocks	408
7.4.4. Variation of the total rate	409
7.5. Multidimensional turbocodes	409
7.6. Bibliography	412
List of Authors	415
Index	417