Monica Borda

Fundamentals in Information Theory and Coding

Springer

Fundamentals in Information Theory and Coding

Monica Borda

Fundamentals in Information Theory and Coding

Springer

Author

Prof. Dr. Eng. Monica Borda
Technical University of Cluj-Napoca
Dept. Communications
Str. Baritiu 26-28
400027 Cluj Napoca
Romania
Telephone: 0040-264401575
E-mail: Monica.Borda@com.utcluj.ro

ISBN 978-3-642-20346-6 e-ISBN 978-3-642-20347-3

DOI 10.1007/978-3-642-20347-3

Library of Congress Control Number: 2011925863

Typeset & Cover Design: Scientific Publishing Services Pvt. Ltd., Chennai, India.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

To my family

Preface

Motto: *We need to develop thinking, rather than too much knowledge.*
Democritus

This book represents my 30 years continuing education courses for graduate and master degree students at the Electronics and Telecommunications Faculty from the Technical University of Cluj Napoca, Romania and partially my research activity too. The presented topics are useful for engineers, M.Sc. and PhD students who need basics in information theory and coding.

The work, organized in five Chapters and four Appendices, presents the fundamentals of Information Theory and Coding.

Chapter 1 (Information Transmission Systems - ITS) is the introductory part and deals with terminology and definition of an ITS in its general sense (telecommunication or storage system) and its role.

Chapter 2 (Statistical and Informational Model of an ITS) deals with the mathematical and informational modeling of the main components of a digital ITS: the source (destination) and the transmission channel (storage medium). Both memoryless and memory (Markov) sources are analyzed and illustrated with applications.

Chapter 3 (Source Coding) treats information representation codes (from the numeral system to the genetic code), lossless and lossy (DPCM and Delta) compression algorithms. The main efficiency compression parameters are defined and a detailed presentation, illustrated with many examples, of the most important compression algorithms is provided, starting with the classical Shannon-Fano or Huffman until the modern Lempel Ziv or arithmetic type.

Chapter 4 (Cryptography Basics) is presenting basics of classic and modern symmetric and public key cryptography. Introduction in DNA cryptography and in digital watermarking are ending the chapter. Examples are illustrating all the presented chipers.

Chapter 5 (Channel Coding) is the most extended part of the work dealing with error control coding: error detecting and forward error correcting codes. After defining the aim of channel coding and ways to reach it as established by Shannon second theorem, the elements of the theory of block codes are given and Hamming group codes are presented in detail.

Cyclic codes are a main part of Chapter 5. From this class, a detailed presentation of BCH, Reed-Solomon, Golay and Fire codes is given, with linear feedback shift register implementation. The algebraic decoding algorithms, Peterson and Berlekamp, are presented.

Concerning the convolutional codes, after a short comparison with block codes, a detailed description of encoding and graphical representation as well as decoding algorithms are given.

Principles of interleaving and concatenation are also presented and exemplified with the CIRC standard used in audio CD error control.

The principles of the modern and powerful Turbo Codes are ending the presentation of error control codes. Channel Coding chapter also includes a presentation of Base-Band coding.

The work also includes four Appendices (A, B, C and D) presenting: A – Algebra elements and tables concerning some Galois fields and generator polynomials of BCH and RS codes; B – Tables for information and entropy computing; C – Signal detection elements and D – Synthesis example.

I tried to reduce as much as possible the mathematical demonstrations, focusing on the conditions of theorems validity and on their interpretation. The examples were selected to be as simple as possible, but pointing out the essential aspects of the processing. Some of them are classic, others are taken from the literature, being currently standards in many real applications, but most of them are original and are based on typical examples taken from my lectures.

The understanding of the phenomenon, of the aims of processing (compression, encryption and error control) in its generality, not necessarily linked to a specific application, the criteria of selecting a solution, the development of the “technical good sense”, is the logic thread guiding the whole work.

Acknowledgements

I want to thank to all those who directly or indirectly, contributed to my training as an engineer and professor.

Special thanks are addressed to Professor Alexandru Spataru and to the school he created. He was my teacher in Theory of Information Transmission, during the time I was student at Polytechnic Institute of Bucharest.

For the interest shown towards the modern algebraic decoding algorithms, for the simplicity and practical way in which he presented the abstract mathematics, I thank professor mathematician Nicolae Ghircoiasu, now pastaway.

I am highly grateful to Dr. Graham Wade, from the University of Plymouth, UK, for the modern and practical orientation he gave to my whole course, for the valuable discussions and fruitful collaboration we had since 1993. His books impressed me a lot, due to the practical features that he gave to a domain usually presented theoretically.

Special thanks are given to my colleagues, professor Romulus Terebeş, teaching assistant Raul Malutan and researcher Bogdan Belean for their observations and suggestions, and to my PhD student Olga Tornea for her contributions to DNA cryptography.

I kindly acknowledge to all students who helped me in typewriting the book.

Chapter 3 and 4 were partially supported by the Romanian National Research Council CNCSIS-UEFISCSU project no. PNII ID_909/2007.

I would like to thank Dr. Christoph Baumann, Senior Editor Engineering at Springer (Germany), who motivated me in preparing the book. Finally, but not least, I thank Carmen Wolf, Editorial Assistant at Springer (Germany) and Ganesan Prabu from Scientific Publishing Services (India) for their wonderful help in the preparation and publication of the manuscript.

Contents

1 Information Transmission Systems 1
1.1 Terminology 1
1.2 Role of an ITS 2
1.3 Model of an ITS 3
References 5

2 Statistical and Informational Model of an ITS 7
2.1 Memoryless Information Sources 7
2.2 Measure of Discrete Information 8
2.3 Information Entropy for a DMS (Shannon Entropy) 11
2.4 Source Redundancy and Efficiency 13
2.5 Entropy of an Extended Discrete Memoryless Source: H(Xn) 14
2.6 Moments and Moment Rate 14
2.7 Information Rate, Decision Rate 15
2.8 Discrete Transmission Channels 16
2.8.1 Probabilities and Entropies in Discrete Channels 16
2.8.2 Mutual Information and Transinformation 21
2.8.3 Relationships between Entropies 21
2.8.4 Channel Capacity Using the Noise Matrix 23
2.8.5 Shannon Capacity 30
2.9 Memory Sources (Markov Sources) 38
2.9.1 Finite and Homogeneous Markov Chains 39
2.9.2 Entropy of m-th Order Markov Source 43
2.9.3 Applications 46
References 51

3 Source Coding 53
3.1 What Is Coding and Why Is It Necessary? 53
3.2 Aim of Source Coding 55
3.3 Information Representation Codes 55
3.3.1 Short History 55
3.3.2 Numeral Systems 56
3.3.3 Binary Codes Used in Data Transmission, Storage or Computing 58

3.3.4 Pulse Code Modulation (PCM) 65
3.3.5 Genetic Code 76
3.4 Coding Efficiency: Compression Ratio 80
3.5 Existence Theorem for Instantaneous and Uniquely Decodable Codes (Kraft and McMillan Inequalities) 82
3.6 Shannon First Theorem (1948) 84
3.7 Losseless Compression Algorithms 85
3.7.1 Shannon-Fano Binary Coding 85
3.7.2 Huffman Algorithms 88
3.7.3 Run Length Coding (RLC) 95
3.7.4 Comma Coding 100
3.7.5 Dictionary Techniques [41] 101
3.7.6 Lempel-Ziv Type Algorithms (LZ) 102
3.7.7 Arithmetic Coding 107
3.8 Lossy Compression in Differential Coding 109
3.8.1 Differential Pulse Code Modulation (DPCM) 109
3.8.2 Delta Modulation (DM) 111
3.8.3 Delta-Sigma Modulation 115
3.8.4 Comparison and Applications of Digital Modulations 116
3.9 Conclusions on Compression 116
References 118

4 Cryptography Basics 121
4.1 Short History of Cryptography 121
4.2 Terminology 123
4.3 Cryptosystems: Role and Classification 123
4.4 Cryptanalytic Attacks and Algorithms Security 125
4.5 Classic Cryptography 127
4.5.1 Definition and Classification 127
4.5.2 Caesar Cipher 128
4.5.3 Polybius Cipher 130
4.5.4 Playfair Cipher 131
4.5.5 Trithemius Cipher 132
4.5.6 Vigénère Cipher 134
4.6 Modern Symmetric (Conventional) Cryptography 135
4.6.1 Definitions and Classification 135
4.6.2 Block Ciphers 137
4.6.2.1 Main Features 137
4.6.2.2 DES (Data Encryption Standard) 139
4.6.2.3 Some Other Block Ciphers 147
4.6.2.4 Block Cipher Operation Modes 150
4.6.3 Stream Ciphers 153
4.6.3.1 General Features 153
4.6.3.2 Some Stream Ciphers 157
4.6.4 Authentication with Symmetric Cryptography 158

4.7 Public Key Cryptography 159
4.7.1 Principle of the Public Key Cryptography 159
4.7.2 Public Keys Ciphers 162
4.8 Digital Watermarking 164
4.8.1 Introduction 164
4.8.2 Short History 167
4.8.3 Watermarking Requirements 168
4.8.4 Basic Principles of Watermarking 169
4.8.5 Specific Attacks 177
4.8.5.1 Attack Definition and Classification 177
4.8.5.2 The Inversion Attack / IBM / Confusion / Deadlock / Fake Watermark / Fake Original 178
4.8.5.3 The Collusion Attack 180
4.8.6 Applications 181
4.8.6.1 Broadcast Monitoring 181
4.8.6.2 Owner Identification: Proof of Ownership 182
4.8.6.3 Fingerprinting (Transaction Tracking) 183
4.8.6.4 Content Authentication (Fragile Watermarking) 183
4.8.6.5 Copy Control 184
4.8.7 The Millennium Watermark System [53] 184
4.8.7.1 Introduction 184
4.8.7.2 Basic Principle of the Millennium System 185
4.8.7.3 Millennium Standard Implementation 188
4.8.7.4 Unsolved Problems 188
4.8.7.5 Copy Control [53] 189
4.8.7.6 Media Type Recognition 189
4.8.8 Some Remarks 189
4.9 DNA Cryptography 190
4.9.1 Introduction 190
4.9.2 Backgrounds of Biomolecular Technologies 190
4.9.3 Elements of Biomolecular Computation (BMC) 194
4.9.3.1 DNA OTP Generation 194
4.9.3.2 Conversion of Binary Data to DNA Format and Vice Versa 194
4.9.3.3 DNA Tiles and XOR with DNA Tiles 195
4.9.4 DNA Based Steganography and Cryptographic Algorithms 197
4.9.4.1 Steganography Technique Using DNA Hybridization 197
4.9.4.2 Chromosome DNA Indexing Algorithm 199
4.9.4.3 DNA XOR OTP Using Tiles 202
References 204

5 Channel Coding 209
5.1 Shannon Second Theorem (Noisy Channels Coding Theorem) 209
5.2 Error Control Strategies 213

5.3 Classification of Error Control Codes 216
5.4 Representation of Binary Code Sequences 216
5.5 Parameters of Detecting and Error Correcting Codes 218
5.6 Maximum Likelihood Decoding (MLD) 220
5.7 Linear Block Codes 224
5.7.1 Linear Block Codes: Definition and Matrix Description 224
5.7.2 Error Syndrome 227
5.7.3 Dimensioning of Error Correcting Linear Block Codes 228
5.7.4 Perfect and almost Perfect Codes 228
5.7.5 Detection and Correction Capacity: Decoded BER 229
5.7.6 Relations between the Columns of H Matrix for Error Detection and Correction 230
5.7.7 Standard Array and Syndrome Decoding 232
5.7.8 Comparison between Linear Error Detecting and Correcting Block Codes 235
5.7.9 Hamming Group Codes 238
5.7.10 Some Other Linear Block Codes 253
5.8 Cyclic Codes 255
5.8.1 Definition and Representation 256
5.8.2 Algebraic Encoding of Cyclic Codes 257
5.8.3 Syndrome Calculation and Error Detection 265
5.8.4 Algebraic Decoding of Cyclic Codes 269
5.8.5 Circuits for Cyclic Encoding and Decoding 274
5.8.6 Cyclic One Error Correcting Hamming Code 286
5.8.7 Golay Code 290
5.8.8 Fire Codes 292
5.8.9 Reed–Solomon Codes 295
5.9 Convolutional Codes 312
5.9.1 Representation and Properties 312
5.9.2 Convolutional Codes Encoding 314
5.9.3 Graphic Representation of Convolutional Codes 320
5.9.4 Code Distance and d_∞ 324
5.9.5 Decoding (Viterbi Algorithm, Threshold Decoding) 326
5.10 Code Interleaving and Concatenation 340
5.10.1 Interleaving 340
5.10.2 Concatenated Codes 342
5.11 Turbo Codes 346
5.11.1 Definition and Encoding 346
5.11.2 Decoding 348
5.11.2.1 Basic Principles 348
5.11.2.2 Viterbi Algorithm (VA) [46], [48] 349
5.11.2.3 Bidirectional Soft Output Viterbi Algorithm (SOVA) [46] 357
5.11.2.4 MAP Algorithm 364
5.11.2.5 MAX-LOG-MAP Algorithm 372

5.11.2.6 LOG-MAP Algorithm 373
5.11.2.7 Comparison of Decoding Algorithms 374
5.12 Line (baseband) Codes 374
References 385

Appendix A: Algebra Elements 389
A1 Composition Laws 389
A1.1 Compositions Law Elements 389
A1.2 Stable Part 389
A1.3 Properties 389
A2 Modular Arithmetic 391
A3 Algebraic Structures 392
A3.1 Group 392
A3.2 Field 393
A3.3 Galois Field 393
A.3.3.1 Field Characteristic 394
A.3.3.2 Order of an Element 395
A4 Arithmetics of Binary Fields 395
A5 Construction of Galois Fields GF(2^m) 398
A6 Basic Properties of Galois Fields, GF(2^m) 402
A7 Matrices and Linear Equation Systems 410
A8 Vector Spaces 412
A8.1 Defining Vector Space 412
A8.2 Linear Dependency and Independency 413
A8.3 Vector Space 414
A9 Table for Primitive Polynomials of Degree k (k max = 100) 417
A10 Representative Tables for Galois Fields GF(2^k) 418
A11 Tables of the Generator Polynomials for BCH Codes 420
A12 Table of the Generator Polynomials for RS Codes 421

Appendix B: Tables for Information and Entropy Computing 427
B1 Table for Computing Values of $-\log_2(x)$, $0.01 \le x \le 0.99$ 427
B2 Table for Computing Values of $-x \cdot \log_2(x)$, $0.001 \le x \le 0.999$ 428

Appendix C: Signal Detection Elements 435
C.1 Detection Problem 435
C.2 Signal Detection Criteria 438
C.2.1 Bayes Criterion 438
C.2.2 Minimum Probability of Error Criterion (Kotelnikov- Siegert) 440
C.2.3 Maximum a Posteriori Probability Criterion (MAP) 441
C.2.4 Maximum Likelihood Criterion (R. Fisher) 441
C.3 Signal Detection in Data Processing (K = 1) 442
C.3.1 Discrete Detection of a Unipolar Signal 442
C.3.2 Discrete Detection of Polar Signal 446

C.3.3 Continuous Detection of Known Signal 448
C.3.4 Continuous Detection of Two Known Signals 453
References 459

Appendix D: Synthesis Example 461

Subject Index...475

Acronyms...483

List of Figures

1.1 Block scheme of a general digital ITS 3
1.2 Illustration of signal regeneration in digital communications: a) original signal, b) slightly distorted signal, c) distorted signal, d) intense distorted signal, e) regenerated signal (l - distance in transmission) 4
2.1 Graphical representation of the entropy corresponding to a binary source 13
2.2 Discrete information sources: a) unipolar binary source (m=2), b) polar binary source (m=2), c) quaternary source (m=4) 15
2.3 Discrete channel: a) graph representation, b) matrix representation..............17
2.4 Graphical representation of the relationships between entropies: a) ordinary channel, b) noiseless channel, c) independent channel 23
2.5 The graph corresponding to a binary erasure channel 26
2.6 Graphical representation of a binary transmission system.............................27
2.7 Illustration of time and amplitude resolutions 31
2.8 Graphical representation of channel capacity 33
2.9 Bandwidth - capacity dependency 34
2.10 Bandwidth-efficiency diagram 35
2.11 Graphical representation of the relations between the information source and the channel 36
2.12 The graph corresponding to a Markov chain with two states 40
2.13 Transition from si to sj in two steps...41
2.14 Absorbent Markov chain 42
2.15 Graph corresponding to a 2-step memory binary source 45
2.16 Differential Pulse Code Modulation for a black-and-white video signal.....49
2.17 Example of burst...50
2.18 The simplified model of a memory channel 50
3.1 Illustration of the transformation S→X realized through encoding...............54
3.2 Coding tree associated to code D from Table 3.1 55
3.3 Block scheme illustrating the generation of PCM signal (PCM modulator and coder)...65
3.4 Block scheme illustrating the receiving PCM process (PCM demodulator / decoder) 65
3.5 Example of PCM generation...66
3.6 Representation of quantisation noise pdf...67
3.7 Companding illustration 71
3.8 Ideal compression characteristic...72
3.9 Threshold effect in PCM systems...75

3.10 DNA structure 77
3.11 The coding tree of Example 3.5 86
3.12 Evolution of dynamic Huffman FGK tree for the message ‘abcbb’ 92
3.13 The effect of one error on the modified Huffman code: a) transmitted sequence, b) and c) received sequence affected by one error 98
3.14 Uniform steps coding for black and white images 100
3.15 Text compression 100
3.16 The LZ-77 algorithm illustration 103
3.17 Illustration of LZ-77 algorithm 104
3.18 Illustration of LZ-78 algorithm 104
3.19 Illustration of DPCM principle 109
3.20 DPCM codec: a) DPCM encoder; b) DPCM decoder 110
3.21 Illustration of the DM 112
3.22 Slope-overload noise 112
3.23 Illustration of granular noise 113
3.24 Granular noise in DM - pdf representation 114
3.25 Delta-Sigma modulation - demodulation block scheme 115
3.26 Classification of compression 116
4.1 Block-scheme of a cryptosystem where: A, B - entities which transmit, receive the information, E - encryption block, D - decryption block, M- plaintext, C - ciphertext, K - cryptographic key block, k_e - encryption key, k_d - decryption key 123
4.2 Illustration of confidentiality 124
4.3 Illustration of authentication 124
4.4 Alberti cipher disk (formula) 132
4.5 Example of P box with n=7 138
4.6 Example of S box with n = 3: a) block scheme, b) truth table 138
4.7 Example of a product cipher (alternation of P and S boxes) 139
4.8 Generation of round keys in DES 142
4.9 DES encryption routine 144
4.10 DES encryption/decryption function f 145
4.11 Illustration of whitening technique: a- encryption, b- decryption 149
4.12 ECB mode: a) encryption; b) decryption 150
4.13 CBC mode : a) encryption, b) decryption 152
4.14 CFB mode: encryption 152
4.15 OFB mode : encryption 153
4.16 Block scheme of a pseudo-noise generator using LFSR 154
4.17 Pseudo-noise generator with LFSR and $g(x)=x^3+ x^2 +1$ 155
4.18 Pseudo noise sequences generator implemented with two LFSRs 156
4.19 Nonlinear multiplexed system for generating pseudo-noise sequences 157
4.20 Block scheme of a public key system 159
4.21 Confidentiality in public key cryptosystems 160
4.22 Authentication in public key cryptosystems 160
4.23 Confidentiality and authentication in public key cryptosystems 161
4.24 Watermark principle block scheme: a) insertion (embedding), b) retrieval / detection 166

4.25 Bloc scheme for watermark insertion 170
4.26 Bloc scheme for watermark extraction and comparison 171
4.27 Line - scanning video signal 173
4.28 Video sequence watermark insertion model 174
4.29 Video sequence watermark extraction model 175
4.30 Millennium Watermark block schemes: a) insertion, b) detection 186
4.31 Hybridization process 191
4.32 Gene representation 191
4.33 Chromosome representation (http://www.ohiohealth.com/) 192
4.34 Amplifying process in PCR technique 192
4.35 Illustration of DNA recombinant process 193
4.36 Illustration of microarray experiment 193
4.37 Binding process between two ssDNA segments 194
4.38 Triple-helix tile 195
4.39 Tiles assembling through complementary sticky ends 196
4.40 Tiles for START bits in a string 196
4.41 Stacks with tiles for the rest of the bits in a string 196
4.42 XOR computation with tiles 197
4.43 Cipher text hiding: a) structure of cipher text inserted between two primers; b) dsDNA containing (hidden) the cipher text 198
4.44 Illustration of OTP scanning process for message encryption 200
4.45 Design of the One Time Pad tiles 203
4.46 Example of message tiles binding 204
4.47 Design of the one-time-pad tiles 204
5.1 Error exponent graphic 210
5.2 Input/output representation of a BSC obtained for C2 211
5.3 Illustration of the relations between information bits and coded ones 212
5.4 Location of channel coding block in a complete transmission (storage) system 213
5.5 ARQ systems for N = 5: a) SW(Stop and Wait); b) GBN(go back N); c) SR(selective repeat) 215
5.6 Minimum distance decoder principle (d=5) 222
5.7 Coding gain representation 238
5.8 Shortened Hamming code for 16 bits memory protection 244
5.9 Hamming (7,4) code block scheme: a) encoding unit; b) decoding unit 247
5.10 HDLC frame format 268
5.11 LFSR with external modulo 2 adders 274
5.12 LFSR with internal modulo 2 adders 276
5.13 Cyclic systematic encoder with LFSR and external modulo two adders 277
5.14 Cyclic systematic encoder with LFSR and internal modulo two adders 279
5.15 Cyclic encoder with LFSR and external $\oplus$: a) block scheme; b) operation table for $g(x)= x^3 + x + 1$ and $m = 4$ 280
5.16 Cyclic encoder with LFSR and internal $\oplus$: a) block scheme; b) operation table for $g(x)= x^3 + x + 1$ and $m = 4$ 281
5.17 Error detection cyclic decoder with LFSR and external $\oplus$ 282
5.18 Error detection cyclic decoder with LFSR and internal $\oplus$ 283

5.19 a) Block scheme and b) the operating table of the cyclic decoder for $g(x) = x^3 + x + 1$ 284
5.20 a) Block scheme and b) the operation table of a cyclic error detection decoder with LFSR and internal $\oplus$ 285
5.21 General block scheme of an error correction cyclic decoder 286
5.22 a) SR block scheme and b) operation of the cyclic decoder from Fig. 5.21, for the cyclic Hamming code (7,4) with $g(x) = x^3 + x + 1$; LFSR with external $\oplus$ 289
5.23 a) SR block scheme and b) operation of the cyclic decoder from Fig. 5.21, for the cyclic Hamming code (7,4) with $g(x) = x^3 + x + 1$; LFSR with internal $\oplus$ 290
5.24 Block schemes for Fire code with $g(x) = x^{10} + x^7 + x^2 + 1$ and $p = 3$: a) encoder and b) decoder 294
5.25 Flow-chart corresponding to Berlekamp-Massey algorithm 307
5.26 Summating circuit over $GF(2^k)$ 309
5.27 Multiplying circuit with α over $GF(2^4)$ 310
5.28 CD player – block scheme 311
5.29 Comparison between block and convolutional codes 313
5.30 Block scheme of: a) systematic and b) non systematic convolutional encoder; (ISR - Information Shift Register) 315
5.31 Representation of the information at: a) encoder input; b) systematic encoder output; c) non-systematic encoder output 316
5.32 a) Convolutional systematic encoder - block scheme and operation; b) Convolutional non-systematic encoder - block scheme and operation 319
5.33 State diagram of the convolutional code with R = 1/2, K = 3 for a) systematic and b) non-systematic type 321
5.34 The graph corresponding to the systematic convolutional code R = 1/2, K = 3; — the encoded structure for i = [0 1 1 0 1] 322
5.35 Trellis corresponding to the convolutional code R = 1/2, K = 3: a) systematic with $g(x) = 1 + x^2$; b) systematic with $g(x) = 1 + x + x^2$; c) non-systematic with $g_1(x) = 1 + x^2$, $g(x) = 1 + x + x^2$ 323
5.36 Viterbi algorithm example for non-systematic convolutional code with R=1/2, K=3, $g_1(x)=1+x^2$, $g_2(x)=1+x+x^2$, on variable number of frames: N=3÷12 328
5.37 Viterbi decoding process for a three error sequence in the first constraint length 332
5.38 Graphical illustration of the hard decision (with 2 levels) and the soft decision (with 8 levels) 333
5.39 Block-scheme of a threshold decoding system 334
5.40 Threshold decoder for the direct orthogonal code R = 1/2, $g_2(x)=1 + x^2 + x^5 + x^6$ 337
5.41 Threshold decoder for indirect orthogonal code R = 1/2, $g_2(x)=1 + x^3 + x^4 + x^5$ 339
5.42 Interleaving example: a) 4 codewords (of length 5) non-interleaved succession; b) interleaved succession (b = burst error length) 340

5.43 Block interleaving....341
5.44 Block-scheme of a convolutional interleaving made with shift registers (C-encoder for independent errors; dC-decoder for independent errors; I – interleaver; dI – de-interleaver)....342
5.45 Block scheme of a concatenated system....342
5.46 Block-scheme of an interleaved concatenated system (C_2 - RS + C_1 - convolutional)....343
5.47 Block scheme of CIRC system....344
5.48 Encoding and interleaving in CIRC system: a) I_1 - even samples B_{2p} are separated from the odd ones B_{2p+1} with 2Tf ; b) C_2 - RS (28,24) encoding; c) I_2 - samples are delayed with different time periods to spread the errors; d) C_1 -RS (32, 28) encoding; e) I_3 - even samples ($B_{2p,i}$) cross interleaving with the next frame odd samples ($B_{2p+1,i+1}$)....344
5.49 Illustration of the decoding process in CIRC system....345
5.50 Basic RSC code: R=1/2, g_0 - feedback polynomial, g_1- feed forward polynomial....347
5.51 Basic turbo transmitter: turbo encoder with R=1/3, BPSK modulation and AWGN channel....348
5.52 Basic turbo-decoder....349
5.53 RSC encoder with R = 1/2 and K=2: a) block- scheme; b) state-diagram; c) trellis:— i=0 input, i=1 input....352
5.54 Trellis representation on τ=4 frames of RSC code with R=1/2 and K=2....360
5.55 Forward recursion; the thick line is representing the ML path (with minimum path metric 0.04)....362
5.56 The backward recursion; ML path is presented with thick line....363
5.57 MAP decoding illustration: a) block scheme of a transmission system with RSC (R = 1/2, K = 3, G = [1, $(1 + x^2)/ (1 + x + x^2)$]) and MAP decoding; b) state transition diagram of RSC encoder with R = 1/2, K = 3, G = [1, $(1 + x^2)/ (1 + x + x^2)$]; c) trellis diagram of RSC code from b)....365
5.58 Graphical MAP representation: a) forward recursion, b) backward recursion....369
5.59 Differential a) encoder and b) decoder....376
5.60 Signal detection: a) block-scheme and b) illustration of BER....381
5.61 Examples of Base Band encoding....384
C.1 Block scheme of a transmission system using signal detection. S- source, N- noise generator, SD- signal detection block, U- user, $s_i(t)$ - transmitted signal, r(t) - received signal, n(t) - noise voltage, $\hat{s}_i(t)$ - estimated signal....435
C.2 Binary decision splits observation space Δ into two disjoint spaces $\Delta 0$ and $\Delta 1$....436
C.3 Block scheme of an optimal receiver (operating according to Bayes criterion, of minimum risk)....438
C.4 Binary detection parameters: P_m- probability of miss, P_D- probability of detection, P_f - probability of false detection....439
C.5 Graphical representation of function Q(y)....440

C.6 Block-scheme of the optimal receiver for unipolar signal and discrete observation 444
C.7 Graphical representation of pdfs of decision variables for unipolar decision and discrete observation 445
C.8 Block Scheme of an optimal receiver with continuous observation decision for one known signal s(t): a) correlator based implementation; b) matched filter implementation....451
C.9 Graphical representation of $p(z/s_0)$ and $p(z/s_1)$ 452
C.10 Observation space in dimensions (r_1, r_2) 455
C.11 Block- scheme of an optimal receiver for continuous decision with two known signal (correlator based implementation)....457
C.12 Representation of the decision process in continuous detection of two known signals 458
D.1 Block-scheme of processing where: 462
D.2 Block scheme of cyclic encoder with LFSR with external modulo two sumators and $g(x) = x^3 + x + 1$ 468
D.3 Non-systematic convolutional encoder for R=1/2 and K=3 ($g^{(1)}(x) = 1 + x + x^2$, $g^{(2)}(x) = 1 + x$) 472

List of Tables

2.1 Prefixes and multiples for bit and byte 10
2.2 Illustration of time and amplitude resolution requirements 37
3.1 Binary codes associated to a quaternary source (M=4) 54
3.2 Conversion between hex, dec, oct and binary numeral systems 58
3.3 Tree corresponding to Morse code 59
3.4 Baudot Code 60
3.5 The 7-bit ISO code (CCITT Nº 5, ASCII). Command characters: -
for national symbols, SP – Space, CR - Carriage Return, LF - Line Feed,
EOT - End of Transmission, ESC – Escape, DEL - Delete 61
3.6 IBM BCD code – 6 bits lenght 62
3.7 EBCDIC code 63
3.8 Binary natural and Gray 4 bits length codes representation...........................64
3.9 Example of 3 bit code in BN and Gray representation 64
3.10 Genetic code – encoding table 78
3.11 Genetic code – decoding table 78
3.12 Modified Huffman code used in fax 97
3.13 LZW algorithm applied to Example 3.14 106
4.1 Classification of classic ciphers 128
4.2 Caesar cipher 129
4.3 Polybius square 130
4.4 Illustration of Playfair cipher 131
4.5 Tabula recta of Trithemius cipher 133
4.6 Vigénère encryption with key word...134
4.7 Vigénère encryption with trial- key letter and plaintext keyword 135
4.8 Vigénère encryption with trial-key and ciphertext keyword........................135
4.9 DNA to binary conversion 194
4.10 Truth table of XOR function...197
5.1 Standard array for a C(n,m) code..232
5.2 Standard array for C(5,3)...233
5.3 Syndrome decoding for a linear code C(n,m) 234
5.5 Syndrome-decoding table for Hamming (7,4) code.......................................248
5.4 Standard array for the Hamming (7,4) code 249
5.6 Encoding table for the cross parity check code..254
5.7 Table of primitive polynomials up to degree $k = 5$ 260
5.8 BCH codes generator polynomials up to $n = 31$ 261
5.9 $GF(2^4)$ generated by $p(x)= x^4+x+1$ 263
5.10 Coefficients of the error polynomials for BCH codes 272

5.11 Cyclic encoder with LFSR and external modulo two adders 278
5.12 σ_t coefficients of the error polynomial for RS codes 299
5.13 Y_k coefficients for RS codes (t=1,2) 300
5.14 d_∞ for the systematic and non-systematic codes: R = 1/2 and K$\in$ [2, 8] ... 326
5.15 The most important direct orthogonal codes [47] for R = 1/2 338
5.16 The most important indirect orthogonal codes for R = 1/2 339
5.17 Example of differential coding 376
A.1 Minimal polynomials for GF(2^3) and generating polynomial
$1 + X + X^3$ 407
A.2 Minimal polynomials for GF(2^4) and generating polynomial
$1 + X + X^4$ 407
A.3 Minimal polynomials for GF(2^5) and generating polynomial
$1 + X + X^5$ 408
D.1 Operation of the encoder from Fig. D.1 for the binary stream i
(the output of the compression block) 473

Chapter 1
Information Transmission Systems

Motto: *When desiring to master science, nothing is worst than arrogance and more necessary than time.*
Zenon

1.1 Terminology

We call *information* "any message that brings a specification in a problem which involves a certain degree of uncertainty" [9]. The word information derived from the ancient Greek words "eidos" (idea) and "morphe" (shape, form), have thus, the meaning of form/shape of the mind.

Taking this definition into consideration we may say that *information* is a fundamental, abstract notion, as energy in physics.

Information has sense only when involves two correspondents: one generating it (the information source S) and another receiving it (the destination D, or the user U). Information can be transmitted at distance or stored (memorized) for later reading. The physical medium, including the contained equipment, that achieves the remote transmission of the information from S to D, is called *transmission channel* C; in the case of storage systems the channel is replaced by the *storage medium*, e.g. CD, tape etc.

Information is an abstract notion. This is why, when stored or transmitted, it must be embedded into a physical form (current, voltage, electromagnetic wave) able to propagate through the channel or to be stored. What we call *signal* is precisely this physical embodiment carrying information.

Remark

Generally speaking, by signal we understand any physical phenomenon able to propagate itself through a medium. One should notice that this definition is restrictive: it rules out the signal that interferes with the information-carrying signal (useful signal); this signal is known as *noise* or *perturbation* (N).

The information source can be discrete (digital source), or continuous (signal source). The discrete source generates a finite number of symbols (e.g. 0 and 1 used in digital communications) while the continuous source, an infinite number of symbols (e.g. voice, television signal, measurement and control signals).

Remark
The sources, as well the destinations, are supposed to have transducers included. By *Information Transmission System (ITS)* we will understand the ensemble of interdependent elements (blocks) that are used to transfer the information from source to destination.

Remarks

- When transmitting the information from source to a remote destination through a channel, we deal with a *transmission system*; on the other hand, when storing the information, we deal with a *storage system.* The problems met in information processing for storage are similar in many aspects to those from transmission systems; therefore in the present work the term information transmission system (ITS) will be used for the general case (transmission as well storage system).
- The signal, as well as the noise, are assumed to be random.

1.2 Role of an ITS

The role of an ITS is to ensure a high degree of fidelity for the information at destination, regardless to the imperfections and interferences occurring in the channel or storage medium. The accuracy degree is estimated using a fidelity criterion, as follows:

For analogue systems:

- *mean squared error* ε:

$$\varepsilon =: \overline{[x(t) - y(t)]^2} \tag{1.1}$$

where x(t), y(t) are the signals generated by the source respectively received at destination; the symbol "______" indicates the time averaging.

- *signal/noise ratio (SNR)* ξ:

$$\xi =: \frac{\overline{[y(t)]^2}}{\overline{[n(t)]^2}} \tag{1.2}$$

where n(t) indicates the noise.

For digital systems:

- *bit error rate (BER)*: the probability of receiving an erroneous bit

The degree of signal processing for transmission or storage, depends on the source, destination, channel (storage medium), the required accuracy degree, and the system cost.

When the source and destination are human beings, the processing may be reduced due to the physiological thresholds (hearing and vision), and also to the human brain processing, requiring a lower degree of fidelity.

When dealing with data transmissions (machines as source and destination), the complexity of processing increases in order to achieve the required fidelity.

For high quality data transmission/storage we may as well improve the channel (storage medium), the choice of the used method being made after comparing the price of the receiver (the equipment used for processing) with the price of the channel (storage medium). The constant decrease of the LSI and VLSI circuits prices justifies the more and more increasing complexity of the terminal equipment, the ultimate purpose being the achievement of high quality transmission/storage.

Remark
In what follows we will exclusively analyze the numerical (digital) transmission systems taking into consideration their present evolution and the future perspectives that show their absolute supremacy even for applications in which the source and the destination are analogue (e.g. digital television and telephony).

1.3 Model of an ITS

The general block scheme of an ITS is presented in Fig. 1.1 which shows the general processing involving information: coding, modulation, synchronization, detection.

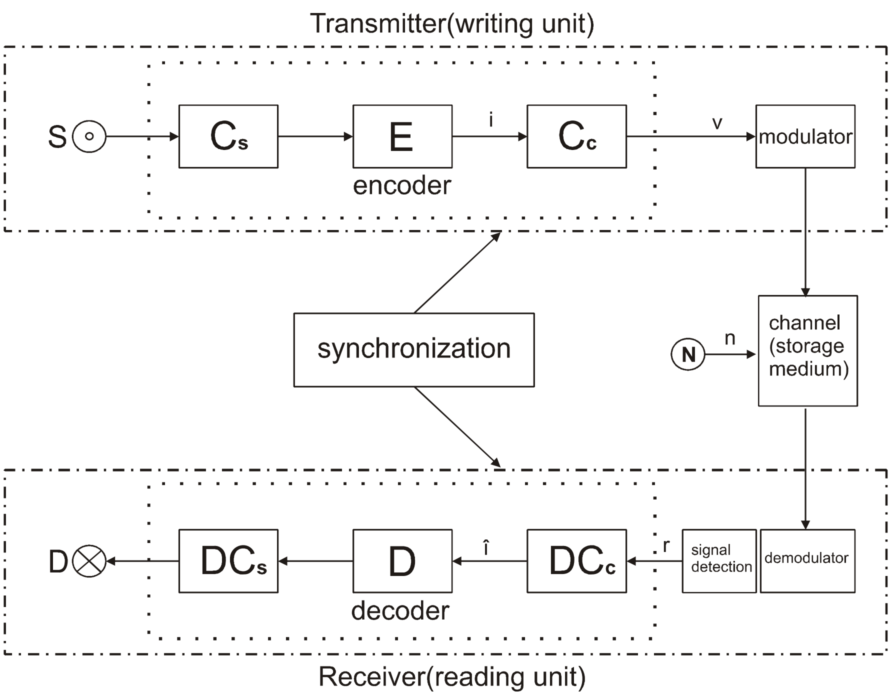

Fig. 1.1 Block scheme of a general digital ITS

Legend:

- S/D – source/destination;
- C_S/ DC_S – source encoding/decoding blocks;
- E/D – source encryption/decryption blocks;

- C_C/DC_C – channel encoding/decoding blocks;
- i – information (signal)
- v – encoded word
- n – noise
- r – received signal
- î – estimated information.

The process named *coding* stands for both encoding and decoding and is used to achieve the followings:

- matching the source to the channel/storage medium (if different as nature), using the source encoding block (C_S)
- ensuring efficiency in transmission/storage, which means minimum transmission time/minimal storage space, all these defining source compression (C_S)
- reliable transmission/storage despite channel/storage medium noise (error protection performed by the channel coding block C_C)
- preserving information secrecy from unauthorized users, using the source encryption/decryption blocks (E/D)

Modulation is used to ensure propagation, to perform multiple access and to enhance the SNR (for angle modulation), as well as to achieve bandwidth compression [8], [25].

For digital systems, *synchronization* between transmitter and receiver is necessary, and also *signal detection*, meaning that the receiver must decide, using the received signal, which of the digital signals has been sent [10].

In real applications, all the above-mentioned processes or only some of them could appear, depending on the processing degree required by the application.

Why digital?

There are several reasons why digital systems are widely used. Their main advantage is high noise immunity, explained by signal regeneration: a digital signal, having only two levels corresponding to “0” and “1”, allows an easy regeneration of the original signal, even from a badly damaged signal (fig.1.2), without accumulation of regenerative errors in transmission (in contrast to analogue transmission) [5], [18].

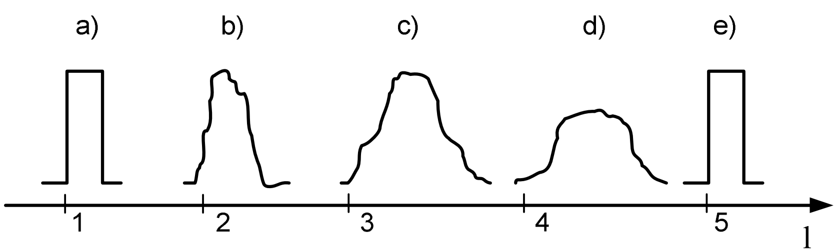

Fig. 1.2 Illustration of signal regeneration in digital communications: a) original signal, b) slightly distorted signal, c) distorted signal, d) intense distorted signal, e) regenerated signal (l - distance in transmission).

In analogue systems, the distortions, however small, cannot be eliminated by amplifiers (repeaters), the noise accumulating during transmission; therefore in order to ensure the required fidelity for a specific application, we must use a high SNR, unlike for digital systems in which (taking into account the possibility of error protection) we may use a very low SNR (lower than 10 dB, near Shannon limit [2]).

Other advantages of digital systems are:

- possibility of more flexible implementation using LSI and VLSI technologies
- reliability and lower price than for analogue systems
- identical analysis in transmission and switching for different information sources: data, telegraph, telephone, television, measurement and control signals (the principle of ISDN – Integrated Switching Digital Network)
- good interference and jamming protection and also the possibility of ensuring information confidentiality.

The main disadvantage of digital systems is the increased bandwidth compared to analogue ones. This disadvantage can be diminished through compression as well as through modulations, for spectrum compression.

References

[1] Angheloiu, I.: Teoria Codurilor. Editura Militara, Bucuresti (1972)
[2] Berrou, C., Glavieux, A.: Near Shannon limit error-correcting coding and decoding turbo-codes. In: Proc. ICC 1993, Geneva, pp. 1064–1070 (1993)
[3] Borda, M.: Teoria Transmiterii Informatiei. Editura Dacia, Cluj-Napoca (1999)
[4] Borda, M.: Information Theory and Coding. U.T. Pres, Cluj-Napoca (2007)
[5] Fontolliet, P.G.: Systhèmes de télècommunications. Editions Georgi, Lausanne (1983)
[6] Gallager, R.G.: Information Theory and Reliable Communication. John Wiley & Sons, Chichester (1968)
[7] Hamming, R.: Coding and Information Theory. Prentice-Hall, Englewood Cliffs (1980)
[8] Haykin, S.: Communication Systems, 4th edn. John Wiley & Sons, Chichester (2001)
[9] Ionescu, D.: Codificare si coduri. Editura Tehnica, Bucuresti (1981)
[10] Kay, S.M.: Fundamentals of Statistical Signal Processing. In: Detection Theory, vol. II. Prentice-Hall, Englewood Cliffs (1998)
[11] Lin, S., Costello, D.: Error Control Coding. Prentice-Hall, Englewood Cliffs (1983)
[12] Mateescu, A., Banica, I., et al.: Manualul inginerului electronist, Transmisii de date. Editura Tehnica, Bucuresti (1983)
[13] McEliece, R.J.: The Theory of Information and Coding, 2nd edn. Cambridge University Press, Cambridge (2002)
[14] Murgan, A.: Principiile teoriei informatiei in ingineria informatiei si a comunicatiilor. Editura Academiei, Bucuresti (1998)
[15] Peterson, W.W., Weldon, E.J.: Error-Correcting Codes, 2nd edn. MIT Press, Cambridge (1972)
[16] Proakis, J.: Digital Communications, 4th edn. Mc Gran-Hill (2001)

[17] Shannon, C.E.: A Mathematical Theory Of Communication. Bell System Technical Journal 27, 379–423 (1948); Reprinted in Shannon Collected Papers, IEEE Press (1993)
[18] Sklar, B.: Digital Communications, 2nd edn. Prentice-Hall, Englewood Cliffs (2001)
[19] Spataru, A.: Teoria transmisiunii informatiei. Editura Didactica si Pedagogica, Bucuresti (1983)
[20] Spataru, A.: Fondements de la theorie de la transmission de l'information. Presses Polytechniques Romandes, Lausanne (1987)
[21] Tomasi, W.: Advanced Electronic Communications. Prentice-Hall, Englewood Cliffs (1992)
[22] Wade, G.: Signal Coding and Processing. Cambridge University Press, Cambridge (1994)
[23] Wade, G.: Coding Techniques. Palgrave (2000)
[24] Wozencraft, J.W., Jacobs, I.M.: Principles of Communication Engineering. Waveland Press, Prospect Heights (1990)
[25] Xiong, F.: Digital Modulation Techniques. Artech House, Boston (2000)

Chapter 2
Statistical and Informational Model of an ITS

Motto: *Measure is the supreme well.*
(from the wisdom of the peoples)

2.1 Memoryless Information Sources

Let us consider a *discrete information source* that generates a number of m distinct symbols (messages). The set of all distinct symbols generated by the source forms the *source alphabet*.

A discrete source is called memoryless (*discrete memoryless source DMS*) if the emission of a symbol does not depend on the previous transmitted symbols.

The statistical model of a DMS is a discrete random variable (r.v.) X; the values of this r.v. will be noted as x_i, $i = \overline{1, m}$. By $X=x_i$ we understand the emission of x_i from m possible.

The m symbols of a DMS constitute a *complete system of events*, hence:

$$\bigcup_{i=1}^{m} x_i = \Omega \quad \text{and} \quad x_i \cap x_j = \Phi, \forall i \neq j \tag{2.1}$$

In the previous formula, Ω signifies the certain event or the sample space and Φ the impossible event.

Consider $p(x_i) = p_i$ the emission probability of the symbol x_i. All these probabilities can be included in the *emission probability matrix* P(X):

$$P(X) = [p_1 \cdots p_i \cdots p_m], \text{ where } \sum_{i=1}^{m} p_i = 1 \tag{2.2}$$

For a memoryless source we have:

$$p(x_i / x_{i-1}, x_{i-2} \ldots) = p(x_i) \tag{2.3}$$

For the r.v. X, which represents the statistical model for a DMS, we have the *probability mass function* (PMF) of r.v. X:

$$X : \begin{pmatrix} x_i \\ p_i \end{pmatrix}, i = \overline{1, m}, \sum_{i=1}^{m} p_i = 1 \tag{2.4}$$

Starting from a DMS, X, we can obtain a new source, having messages which are sequences of n symbols of the initial source X. This new source, X^n , is called the *n-th order extension of the source X.*

$$X:\begin{pmatrix} x_i \\ p_i \end{pmatrix}, i=\overline{1,m}, \sum_{i=1}^{m} p_i = 1$$

$$X^n:\begin{pmatrix} m_j \\ p_j \end{pmatrix}, j=\overline{1,m^n}, \sum_{j=1}^{m^n} p_j = 1 \tag{2.5}$$

$$\text{where}\begin{cases} m_j = x_{j_1} x_{j_2} \dots x_{j_n} \\ p_j = p(x_{j_1})p(x_{j_2})\dots p(x_{j_n}) \end{cases}$$

The source X^n contains a number of m^n distinct m_j messages formed with alphabet X.

Example 2.1
Consider a binary memoryless source X:

$$X:\begin{pmatrix} x_1 & x_2 \\ p_1 & p_2 \end{pmatrix}, p_1 + p_2 = 1$$

The 2nd order extension (n=2) of the binary source X is:

$$X^2:\begin{pmatrix} x_1x_1 & x_1x_2 & x_2x_1 & x_2x_2 \\ p_1^2 & p_1p_2 & p_2p_1 & p_2^2 \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ p_1^* & p_2^* & p_3^* & p_4^* \end{pmatrix}, \sum_{j=1}^{4} p_j^* = 1$$

2.2 Measure of Discrete Information

As shown in 1.1, information is conditioned by uncertainty (non-determination).

Consider the DMS, $X:\begin{pmatrix} x_i \\ p_i \end{pmatrix}, i=\overline{1,m}, \sum_{i=1}^{m} p_i = 1$. Prior to the emission of a symbol x_i there is an uncertainty regarding its occurrence. After the emission of x_i this uncertainty disappears, resulting the information about the emitted symbol. Information and uncertainty are closely connected, but not identical. They are inversely proportional measures, information being a removed uncertainty. It results that the information varies oppositely to the uncertainty.

The uncertainty regarding the occurrence of x_i depends on its occurrence probability: p_i, the both measures being connected through a function $F(p_i)$ that increases as p_i decreases.

Defining the information $i(x_i)$ as a measure of the a priori uncertainty regarding the realization of x_i, we can write:

$$i(x_i) = F(p_i) \tag{2.6}$$

In order to find a formula for the function F we impose that F carries all the properties that the information must have: