Contents

Preface ix

Chapter 1. The Concept of Logic 1

1.1. Syllogisms 1
1.2. Elementary operations of propositional calculus 5
1.2.1. Negation 5
1.2.2. Conjunction 6
1.2.3. Disjunction 7
1.2.4. Conditional 8
1.2.5. Biconditional 10
1.2.6. Tautologies 10
1.3. Tools of deductive reasoning 14
1.4. Quantification 17
1.5. Prenex forms and pure forms 20

Chapter 2. Sets and Relationships 25

2.1. Generalities 25
2.2. Algebra of sets 29
2.3. Parts and partitions 30
2.4. Cartesian product 31
2.5. Binary relationships 32
2.6. Properties of relationships 35
2.7. Applications 42

Chapter 3. Counting and Combinatorial Analysis 47

3.1. Set cardinals 47
3.2. Permutations, arrangements, combinations 48
3.3. Properties of binomial coefficients 51
3.4. Stirling's formula 54

Chapter 4. Boolean Algebra and Boolean Functions 61

4.1. Special elements of an ordered set 61
4.2. Lattice. 66
4.3. Boolean algebra 68
4.4. Boolean functions 72

Chapter 5. Logic Circuits 75

5.1. Canonical forms of a Boolean function 75
5.2. Reduction of a Boolean function 80
5.3. Karnaugh tables 84
5.4. Elementary logic circuits 87
5.5. A little on electronics 93
5.6. Construction of logical functions. 97
5.7. A basic circuit: the binary adder 100

Chapter 6. Arithmetic 103

6.1. Reminder about integers 103
6.2. Euclidean division 104
6.3. Divisibility and prime numbers. 106
6.4. GCD and LCM. 112
6.5. Congruencies. 116
6.6. Elliptic curves 121
6.7. Identity, theorem and Bézout algorithm 127

Chapter 7. Error Protection 131

7.1. General context 131
7.2. Linear codes 136
7.3. Polynomial codes 140
7.4. Convolutional codes. 142

Chapter 8. Encryption Systems 145

8.1. Substitution and transposition 145
8.2. Substitution methods 147
8.2.1. Replacement of a symbol by a symbol 147
8.2.2. The code: replacement of a word by a word 157
8.3. Transposition methods 158
8.4. Asymmetric systems. 159
8.5. DES – secret key system 160
8.6. RSA – public key system 165
8.7. Cryptography with elliptic curves 167

8.8. Quantum cryptography 169
8.9. Appendix: the Crow and the Fox 176

Chapter 9. Probabilities 177

9.1. Chance 177
9.2. Counting and probabilities 178
9.3. Events and probabilities 183
9.4. Statistics and probabilities 189
9.5. Compound probabilities 191
9.6. Graphs, states, transitions 195
9.7. Markov chains 199
9.7.1. Definition 199
9.7.2. Transition matrix 201
9.7.3. Evolution rules 205
9.7.4. Ergodicity 206

Chapter 10. Descriptive Statistics 213

10.1. Statistical description 213
10.1.1. A little vocabulary 213
10.1.2. Tabular presentation and frequency 215
10.1.3. Two-dimensional series 219
10.2. Graphical representations 220
10.2.1. Bar charts 220
10.2.2. Histograms 222
10.2.3. Cumulative diagrams 223
10.2.4. Polar diagrams 226
10.2.5. Pie charts 227
10.2.6. Figurative diagrams 227
10.2.7. Point clouds 228
10.3. Position parameters 229
10.3.1. Mode 229
10.3.2. Median 230
10.3.3. Averages 235
10.3.4. Comparison of position parameters 237
10.4. Dispersion parameters 238
10.4.1. Range, interquartile range, mean range 238
10.4.2. Variance and standard deviation 240
10.4.3. Coefficient of variation and concentration index 242
10.5. Linear adjustment 243
10.5.1. Principle of adjustment 243
10.5.2. Linear adjustment 248

10.6. Chronological series 254
10.6.1. Introduction 254
10.6.2. Study of the general trend. 257
10.6.3. Study of seasonal variations 260
10.7. Covariance and correlation 265
10.7.1. Regression lines 265
10.7.2. Linear correlation 268

Chapter 11. Probability Laws and Simulation 273

11.1. Random variables 273
11.2. Mathematical expectation, variance and standard deviation 283
11.3. Distribution function 287
11.4. Usual probability laws 289
11.4.1. Uniform law 289
11.4.2. Binomial or Bernoulli's law. 290
11.4.3. Poisson's law 293
11.4.4. Exponential law 294
11.4.5. Normal law. 298
11.5. General information on simulation 305
11.5.1. Weak law of large numbers. 305
11.5.2. Some simulations 308
11.5.3. Generation of random numbers 313
11.6. Generating programs 316
11.6.1. Usual laws 317
11.6.2. Any probability law 318
11.7. M/M/1 waiting system 320
11.7.1. Theoretical study 322
11.7.2. Simulation 326
11.8. Appendices 333
11.8.1. Appendix 1: Table for Poisson's law 333
11.8.2. Appendix 2: Table for normal law 334
11.8.3. Appendix 3: Buffon's needle 335
11.8.4. Appendix 4: Results for M/M/1 337

References. 339

List of Authors 341

Index. 343