Contents

Preface ... V

1 Positioning on Earth and in Space ... 1
- 1.1 Introduction ... 1
- 1.2 Global Positioning System ... 2
  - 1.2.1 Some Facts about GPS ... 2
  - 1.2.2 The Theory Behind GPS ... 3
  - 1.2.3 Dealing with Practical Difficulties. ... 6
- 1.3 How Hydro-Québec Manages Lightning Strikes ... 12
  - 1.3.1 Locating Lightning Strikes ... 12
  - 1.3.2 Threshold and Quality of Detection ... 15
  - 1.3.3 Long-Term Risk Management ... 18
- 1.4 Linear Shift Registers ... 19
  - 1.4.1 The Structure of the Field $\mathbb{F}_2^r$ ... 22
  - 1.4.2 Proof of Theorem 1.4 ... 24
- 1.5 Cartography ... 27
- 1.6 Exercises ... 36

References ... 43

2 Friezes and Mosaics ... 45
- 2.1 Friezes and Symmetries ... 48
- 2.2 Symmetry Group and Affine Transformations ... 52
- 2.3 The Classification Theorem ... 58
- 2.4 Mosaics ... 64
- 2.5 Exercises ... 67

References ... 83

3 Robotic Motion ... 85
3.1 Introduction ... 85
3.1.1 Moving a Solid in the Plane ... 87
3.1.2 Some Thoughts on the Number of Degrees of Freedom ... 89
3.2 Movements That Preserve Distances and Angles ... 91
3.3 Properties of Orthogonal Matrices ... 94
3.4 Change of Basis ... 103
3.5 Different Frames of Reference for a Robot ... 106
3.6 Exercises ... 111

References ... 117

4 Skeletons and Gamma-Ray Radiosurgery ... 119
4.1 Introduction ... 119
4.2 Definition of Two-Dimensional Region Skeletons ... 120
4.3 Three-Dimensional Regions ... 130
4.4 The Optimal Surgery Algorithm ... 132
4.5 A Numerical Algorithm ... 134
4.5.1 The First Part of the Algorithm ... 135
4.5.2 Second Part of the Algorithm ... 139
4.5.3 Proof of Proposition 4.17 ... 140
4.6 Other Applications of Skeletons ... 142
4.7 The Fundamental Property of the Skeleton ... 143
4.8 Exercises ... 147

References ... 153

5 Savings and Loans ... 155
5.1 Banking Vocabulary ... 155
5.2 Compound Interest ... 156
5.3 A Savings Plan ... 159
5.4 Borrowing Money ... 161
5.5 Appendix: Mortgage Payment Tables ... 164
5.6 Exercises ... 168

References ... 171

6 Error-Correcting Codes ... 173
6.1 Introduction: Digitizing, Detecting and Correcting ... 173
6.2 The Finite Field $\mathbb{F}_2$ ... 178
6.3 The $C(7,4)$ Hamming Code ... 179
6.4 $C(2^k-1, 2^k-k-1)$ Hamming Codes ... 182
6.5 Finite Fields ... 185
6.6 Reed–Solomon Codes ... 193

6.7 Appendix: The Scalar Product and Finite Fields . . . 198
6.8 Exercises . . . 200

References . . . 207

7 Public Key Cryptography . . . 209
7.1 Introduction . . . 209
7.2 A Few Tools from Number Theory . . . 210
7.3 The Idea behind RSA . . . 213
7.4 Constructing Large Primes . . . 221
7.5 The Shor Factorization Algorithm . . . 231
7.6 Exercises . . . 234

References . . . 239

8 Random-Number Generators . . . 241
8.1 Introduction . . . 241
8.2 Linear Shift Registers . . . 245
8.3 $\mathbb{F}_p$-Linear Generators . . . 248
8.3.1 The Case $p = 2$ . . . 248
8.3.2 A Lesson on Gambling Machines . . . 253
8.3.3 The General Case . . . 253
8.4 Combined Multiple Recursive Generators . . . 255
8.5 Conclusion . . . 257
8.6 Exercises . . . 258

References . . . 263

9 *Google* and the *PageRank* Algorithm . . . 265
9.1 Search Engines . . . 265
9.2 The Web and Markov Chains . . . 268
9.3 An Improved *PageRank* . . . 278
9.4 The Frobenius Theorem . . . 281
9.5 Exercises . . . 284

References . . . 289

10 Why 44,100 Samples per Second? . . . 291
10.1 Introduction . . . 291
10.2 The Musical Scale . . . 292
10.3 The Last Note (Introduction to Fourier Analysis) . . . 296
10.4 The Nyquist Frequency and the Reason for 44,100 . . . 307
10.5 Exercises . . . 317

References . . . 323

11 Image Compression: Iterated Function Systems 325
11.1 Introduction 325
11.2 Affine Transformations in the Plane 327
11.3 Iterated Function Systems 330
11.4 Iterated Contractions and Fixed Points 336
11.5 The Hausdorff Distance 340
11.6 Fractal Dimension 345
11.7 Photographs as Attractors 350
11.8 Exercises 361

References 367

12 Image Compression: The JPEG Standard 369
12.1 Introduction 369
12.2 Zooming in on a JPEG-Compressed Digital Image 372
12.3 The Case of 2×2 Blocks 373
12.4 The Case of $N \times N$ Blocks 378
12.5 The JPEG Standard 388
12.6 Exercises 396

References 401

13 The DNA Computer 403
13.1 Introduction 403
13.2 Adleman's Hamiltonian Path Problem 405
13.3 Turing Machines and Recursive Functions 409
13.3.1 Turing Machines 409
13.3.2 Primitive Recursive Functions and Recursive Functions 416
13.4 Turing Machines and Insertion–Deletion Systems 426
13.5 NP-Complete Problems 430
13.5.1 The Hamiltonian Path Problem 430
13.5.2 Satisfiability 431
13.6 More on DNA Computers 435
13.6.1 The Hamiltonian Path Problem and Insertion–Deletion Systems 435
13.6.2 Current Limits 435
13.6.3 A Few Biological Explanations Concerning Adleman's Experiment 437
13.7 Exercises 441

References 445

14 Calculus of Variations 447
14.1 The Fundamental Problem of Calculus of Variations 448
14.2 Euler–Lagrange Equation 451
14.3 Fermat's Principle 455
14.4 The Best Half-Pipe. 457
14.5 The Fastest Tunnel 460
14.6 The Tautochrone Property of the Cycloid 465
14.7 An Isochronous Device 468
14.8 Soap Bubbles 471
14.9 Hamilton's Principle 475
14.10 Isoperimetric Problems 479
14.11 Liquid Mirrors 486
14.12 Exercises 490

References 499

15 Science Flashes 501
15.1 The Laws of Reflection and Refraction 501
15.2 A Few Applications of Conics 508
15.2.1 A Remarkable Property of the Parabola 508
15.2.2 The Ellipse 518
15.2.3 The Hyperbola 520
15.2.4 A Few Clever Tools for Drawing Conics 521
15.3 Quadratic Surfaces in Architecture 521
15.4 Optimal Cellular Antenna Placement 528
15.5 Voronoi Diagrams 532
15.6 Computer Vision 537
15.7 A Brief Look at Computer Architecture 539
15.8 Regular Pentagonal Tiling of the Sphere 544
15.9 Laying Out a Highway 551
15.10 Exercises 552

References 567

Index 569