Odile Papini Jacques Wolfmann

Algèbre discrète et codes correcteurs

Springer

Sommaire

Introduction 1

Du bon usage de cet ouvrage 3

PARTIE 1 : HISTORIQUE

Chapitre I. Du télégraphe au disque compact, de l'algèbre de Boole à la géométrie algébrique 7

§1. L'évolution des techniques de transport de messages 7
§2. Le codage de l'information 11
§3. Les codes correcteurs d'erreurs et l'histoire des mathématiques . . 12
§4. Les codes correcteurs d'erreurs et l'histoire de l'informatique . . . 14
§5. La théorie des codes : émergence d'une nouvelle discipline 17
§6. La théorie de l'information 22
§6.2. Le modèle d'un système de communication 23
§6.2. Définition mathématique de l'information 23
§6.4. Le canal de transmission 24
§6.4. Le théorème de Shannon 24

PARTIE 2 : ALGÈBRE

Chapitre II. Equivalences d'applications, ensembles finis 29

§1. Correspondances et relations d'équivalence 29
§2. Fonctions et applications 30
§2.1. Définitions 30
§2.2. Composition des applications, applications réciproques . . . 31
§4. Equivalence d'application, décomposition d'une application 32
§4. Ensembles finis 33
§4.2. Définitions et propriétés élémentaires 33
§4.2. Dénombrement 33

Chapitre III. Groupes 35

§2. Structures 35
§2. Définition des groupes 35
§4. Propriétés élémentaires des groupes 36
§5. Sous-groupes 37
§6. Morphismes de groupes 38

§6. Equivalence d'application d'un morphisme de groupes 38
§7. Groupe quotient par le noyau 39
§8. Sous-groupes distingués, groupes quotients 40
§10. Equivalences associées à un sous-groupe quelconque 41
§11. Ordre et exposant d'un groupe fini 42
§11. Groupes cycliques 43
§11.2. Groupes monogènes, groupes cycliques 43
§11.2. Sous-groupes d'un groupe cyclique 43
§11.3. Générateurs d'un groupe cyclique, équation $x^i = b$ 44

Chapitre IV. Anneaux **45**

§1. Définition et propriétés des anneaux 45
§3. Anneaux intègres 46
§4. Sous-anneaux 47
§4. Morphismes d'anneaux 47
§6. Equivalence d'application d'un morphisme d'anneaux 48
§6. Anneaux quotients 48
§7. Idéaux d'un anneau 49

Chapitre V. Idéaux et morphismes de $\mathbb{Z}$ et de $\mathbb{K}[x]$ **51**

§2. Division (euclidienne) dans $\mathbb{Z}$ 51
§2. Sous-groupes et idéaux de $\mathbb{Z}$ 51
§3. Pgcd, ppcm, Théorème de Bezout 52
§3.1. Plus grand commun diviseur 52
§4.0. Plus petit commun multiple 53
§4. Morphismes de $\mathbb{Z}$, équivalence modulo n 53
§5. L'anneau des entiers modulo n 54
§5.3. Définition 54
§5.3. Eléments inversibles et diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$ 54
§6.0. Application résiduelle modulo n 55
§6. Sous-groupes et idéaux de $\mathbb{K}[X]$ 55
§7. Pgcd, ppcm, Théorème de Bezout pour les polynômes 56
§7.1. Plus grand commun diviseur 56
§8.0. Plus petit commun multiple 57
§8. Morphismes (d'anneaux) de $\mathbb{K}[x]$, équivalence modulo $f(x)$ 57
§9. L'anneau des polynômes modulo $f(x)$ 58
§9.2. Définition 58
§9.2. Eléments inversibles et diviseurs de zéro dans $\mathbb{K}[x]/(f(x))$. 58
§9.3. application résiduelle modulo $f(x)$ 59

Chapitre VI. Construction des corps finis **61**

§1. Corps quotient sur un corps premier 61
§2. Etudes des corps commutatifs finis 62

§2.1. Sous-corps premiers 62
§2.2. Propriétés de la caractéristique 64
§2.4. Groupe multiplicatif 66
§2.4. Polynôme minimal 66
§2.5. Sous-corps $\mathbb{F}_p(\beta)$ 67
§2.7. Cas particulier fondamental 69
§2.7. Théorème de Wedderburn et conclusion 69

Chapitre VII. Théorèmes d'existence **71**

§1. Polynôme irréductible et polynôme minimal 71
§2. Corps de rupture, et corps de décomposition 72
§3. Existence d'un corps de cardinal p^n 73
§4. Description d'un corps fini au moyen d'une racine primitive 75

Chapitre VIII. Sous-corps et automorphismes d'un corps fini **77**

§1. Sous-corps 77
§2. Automorphismes d'un corps fini 78
§2.1. Propriétés des automorphismes 78
§2.2. Automorphismes de Galois 79
§2.3. Conjugaison 80
§3. Détermination de tous les automorphismes d'un corps fini 82

Chapitre IX. Racines de l'unité **85**

§2. Préliminaires 85
§2. Groupe des racines n-ièmes de l'unité dans un corps fini 85
§3. Corps des racines n-ièmes de l'unité sur $\mathbb{F}_p$ 86
§5. Décomposition de $x^n - 1$ sur $\mathbb{F}_p$ 88
§5. Classes cyclotomiques 89
§6. Ordre d'un polynôme 90

PARTIE 3 : CODES CORRECTEURS

Chapitre X. Généralités sur les codes correcteurs **95**

§1. Introduction 95
§3. Définitions 99
§3. Codes correcteurs 100
§3.1. Condition de décodage d'ordre e, rayon de recouvrement . . 100
§3.3. Théorème fondamental 101
§3.3. Borne d'empilement de sphères 101
§4. Codes équivalents 103

Chapitre XI. Codes linéaires 105

§1. Introduction 105
§2. Première description des codes linéaires : Matrices génératrices . 106
§2.1. Définitions et propriétés 106
§2.2. Codage des messages au moyen d'un code linéaire 108
§2.3. Borne de Singleton et codes M.D.S 109
§3.1. Codes simplexes (binaires) 110
§3. Deuxième description des codes linéaires : Matrices de contrôle . 110
§3.1. Définitions et propriétés 110
§3.3. Construction pour un code systématique 111
§3.4. Codes de Hamming (binaires) 112
§3.4. Décodage au moyen d'une matrice de contrôle 112

Chapitre XII. Corps finis et polynômes sur un corps fini 117

§1. Calculs résiduels sur les entiers et les polynômes 117
§1.1. Entiers 117
§1.2. Polynômes 118
§2. Corps finis 119
§3. Construction d'un corps fini au moyen d'un polynôme primitif . . 120
§4. Automorphismes de Galois 121

Chapitre XIII. Codes Cycliques 123

§1. Définition et description 123
§1.1. Représentation polynomiale 124
§1.2. En résumé 125
§2. Dimension et matrice génératrice d'un code cyclique 127
§3. Orthogonal d'un code cyclique 129
§4. Décomposition de $x^n - 1$ sur $\mathbb{F}_q$ 131
§4.1. Premier cas : n est premier avec p 131
§5.0. Deuxième cas : n non-premier avec p 133
§5. Codage systématique d'un code cyclique 133

Chapitre XIV. Les codes B.C.H. 135

§1. Enoncé du théorème des codes B.C.H. 135
§3. Définition des codes B.C.H. 136
§3. Démonstration du théorème 136
§4. Commentaires 137
§5. Première description des codes de Reed-Solomon 138
§6. Deuxième description des codes de Reed-Solomon 139

Chapitre XV. Applications des codes correcteurs dans l'industrie 141

§1. Code utilisé pour le disque compact 141
§1.1. Historique 141

§1.2. Numérisation de l'information 142
§1.3. Préliminaires à la présentation du code C.I.R.C. 143
§3.0. Le code de Reed-Solomon à entrelacement croisé 146
§3. Code utilisé pour le Minitel 146
§3. Utilisation du codage pour la transmission par satellite 147
§3.2. Historique 147
§3.2. Présentation des codes de Reed-Muller 148
§3.3. Quelques codes utilisés pour la transmission d'images . . . 149

Exercices **151**

PARTIE 4 : DÉCODAGE

Chapitre XVI. Décodage des codes linéaires **157**

§2. Généralités 157
§2. Définitions 158
§3. Décodage par tableau de déchiffrement 159
§4. Décodage par décision majoritaire 160
§4.1. Décodage en une étape 160
§5.0. Décodage en plusieurs étapes 165
§5. Décodage par permutations 165

Chapitre XVII. Décodage des codes cycliques **169**

§1. Généralités 169
§2. Décodage de Meggitt 171
§3. Décodage par piégeage d'erreur 175
§4. Décodage algébrique des codes B.C.H. 178
§5. Décodage par transformation de Fourier discrète 186
§5.1. Transformation de Fourier discrète sur les corps finis 186
§5.2. Méthode de décodage par transformation de Fourier 187

PARTIE 5 : COMPLÉMENTS

Chapitre XVIII. Autres pistes et problèmes ouverts **195**

§1. Codes optimaux et classes de bons codes 195
§1.2. Optimisation des paramètres 195
§1.2. Codes M.D.S. 195
§2.0. Les classes de bon codes 196
§3. Codes auto-duaux 197
§3. Groupes et codes 198
§3.2. Groupe d'isométries et groupe d'automorphismes d'un code 198
§3.2. Groupes finis simples et réseaux 198
§4. Idéaux d'algèbre de groupes 199
§6. Rayon de recouvrement 200

§7. Fonctions courbes 201
§7. Codes et configurations combinatoires 201
§7.1. Configurations combinatoires 201
§7.3. Les t-configurations 202
§7.3. Plans projectifs finis 202
§8. Codes et géométrie algébrique, codes de Goppa 203
§9. Equations sur les corps finis 204
§9.2. Codes linéaires binaires 205
§9.2. Codes cycliques 205
§9.4. Les équations fondamentales et les courbes associées 206
§9.4. Equations diagonales 206
§10. Cryptographie 207

Chapitre XIX. Compléments sous forme de problèmes **209**

§1. Trace 209
§3. Norme 210
§4. Bases normales 211
§5. Fonctions sur un corps fini 212
§5. Polynômes linéarisés 212
§7. Codes raccourcis 213
§8. Codes auto-duaux 214
§8. Codes M.D.S. 214
§9. Codes binaires à poids pairs 215
§10. Rayon de recouvrement 216

PARTIE 6 : ANNEXES

Annexe 1 : Rappels d'algèbre linéaire **221**

§2. Sous-espaces 221
§2. Générateurs, bases 221
§3. Applications linéaires 222
§7. Espaces Isomorphes 223
§7. Rang 223
§7. Matrice de Vandermonde 223
§7. Produit scalaire, orthogonalité 224

Annexe 2 : Représentation et algorithmes de calcul dans les corps finis **225**

§2. Représentation polynomiale 225
§2. Puissances d'un élément primitif 226

Annexe 3 : Table de polynômes irréductibles primitifs **229**

Annexe 4 : Tables de corps finis **231**

Annexe 5 : Implémentation du calcul dans les corps finis 241

§1. Arithmétique sur les corps finis 241
§2. Arithmétique sur les polynômes 243
§2.2. Décalage circulaire 243
§2.2. Multiplication de deux polynômes 244
§2.3. Calcul du reste dans la division de deux polynômes 245

Annexe 6 : Transformation de Fourier discrète 247

§1. Transformation de Fourier discrète sur le corps des complexes . 247
§2. Transformation de Fourier discrète sur les corps finis 248
§3. Généralisation 249

Bibliographie. 253

Index 257