

Table des matières

1	Théorie naïve des ensembles, calcul booléen	17
1.1	Ensembles, éléments, appartenance	17
1.2	Inclusion, ensemble des parties	19
1.2.1	Les patates	21
1.2.2	Ensemble des parties	22
1.3	Opérations usuelles dans $\mathcal{P}(E)$	23
1.3.1	Intersection	23
1.3.2	Union ou réunion	23
1.3.3	Différence, différence symétrique, complémentaire	24
1.3.4	Application caractéristique	26
1.3.5	Partition	29
1.4	Produit cartésien	29
1.4.1	Couples, n -uplets	29
1.4.2	Produit cartésien	30
1.4.3	Propriétés	31
1.5	Cardinaux	31
1.6	Calcul booléen	33
2	Relations binaires	49
2.1	Relations binaires entre deux ensembles	49
2.1.1	Domaine, codomaine	50
2.1.2	Représentation d'une relation	51
2.1.3	Relation réciproque	53
2.1.4	Image, contre image d'une partie	54
2.1.5	Égalité de deux relations	54
2.1.6	Restriction, prolongement	55
2.1.7	Négation, inclusion, union, intersection	55
2.1.8	Composition	58
2.2	Fonctions, applications	62
2.2.1	Notion de famille d'éléments	63
2.2.2	Fonctions particulières	64
2.3	Relations n -aires	70
2.4	Relations binaires sur un ensemble	72
2.4.1	Représentations	72
2.4.2	Inclusion, union, intersection et négation	73
2.4.3	Composition	74
2.4.4	Propriétés particulières	79
2.5	Relations d'équivalence	83
2.6	Relations d'ordre	84
2.6.1	Ensembles ordonnés	85
2.7	Treillis	93
2.7.1	Treillis distributif	94
2.7.2	Treillis complémenté	94
2.8	Algèbre de Boole	95

3	Logique des propositions	99
3.1	Introduction	99
3.2	Généralités sur la logique des propositions	99
3.3	Le langage de la logique des propositions	100
3.3.1	Le vocabulaire	100
3.3.2	Les formules	101
3.3.3	Démonstration par induction	102
3.3.4	Sous-formule, arbre de décomposition d'une formule	103
3.4	La sémantique de la logique des propositions	104
3.4.1	Les connecteurs et leur interprétation	104
3.4.2	Distribution des valeurs de vérité, tables de vérité	105
3.4.3	Calcul booléen, dans $\mathbb{Z}/2\mathbb{Z}$ et distribution des valeurs de vérité	107
3.4.4	Classement des formules, les tautologies	110
3.4.5	L'équivalence sémantique	112
3.4.6	Système complet de connecteurs	114
3.4.7	Forme normale conjonctive, clauses	116
3.4.8	Conséquence logique ou sémantique	118
3.5	Un système de preuve	122
3.5.1	La méthode de résolution	122
3.5.2	Brève initiation au langage Prolog	131
4	Logique des prédicats	137
4.1	Introduction	137
4.2	Le langage de la logique des prédicats	139
4.2.1	Le vocabulaire	139
4.2.2	Les termes	141
4.2.3	Les formules	143
4.2.4	Substitution dans une formule	147
4.3	La sémantique de la logique des prédicats	147
4.3.1	Réalisation d'un langage	148
4.3.2	Interprétation d'un terme	149
4.3.3	Satisfaction d'une formule	150
4.3.4	Formules universellement valides, équivalence sémantique	152
4.3.5	Forme prénexe	154
4.3.6	Forme de Skolem	156
4.3.7	Conséquence sémantique	157
4.4	Méthode de résolution	158
5	Langages et automates	163
5.1	Langages	163

5.1.1	Alphabet	163
5.1.2	Chaîne de caractères, mots	163
5.1.3	Monoïde libre	164
5.1.4	Langages	166
5.1.5	Opérations sur les langages	167
5.2	Langages et expressions rationnels	168
5.2.1	Langages rationnels ou réguliers	169
5.2.2	Expressions rationnelles	169
5.3	Grammaires, systèmes formels	171
5.4	Automates à états finis	173
5.4.1	Calculs	176
5.4.2	Automates équivalents	177
5.4.3	Union	177
5.4.4	Produit cartésien	177
5.4.5	États accessibles, coaccessibles	178
5.4.6	Automates émondés	179
5.4.7	Automates complets	180
5.4.8	Automates déterministes	182
5.4.9	Complémentation	184
5.4.10	Automates normalisés	185
5.4.11	Automates avec transitions spontanées	188
5.5	Le théorème de Kleene	189
5.6	Retour aux grammaires	197
5.7	Opérations sur les automates	199
6	Graphes, arbres	201
6.1	Généralités	201
6.2	Graphes simples orientés	203
6.3	Graphes simples non orientés	220
6.4	Arbres, arborescences	221
6.4.1	Arbres	221
6.4.2	Arborescences	222
6.4.3	Arborescences ordonnées	224
6.4.4	Arbres binaires (ordonnés)	225
7	Polynômes	235
7.1	Définitions	235
7.2	Fonction polynôme	236
7.3	Opérations	237
7.4	Schéma de Hörner	240
7.5	Division euclidienne	244
7.6	Décalage circulaire	246
7.7	Polynômes irréductibles	248
7.8	Zéros des polynômes	248
7.9	Anneau quotient	249

7.9.1	Idéaux de $\mathbb{K}[X]$	249
7.9.2	Relation d'équivalence dans $\mathbb{K}[X]$	249
7.9.3	L'anneau $\mathbb{K}[X]/M$	250
7.10	Extension de corps	251
8	Calcul matriciel, systèmes linéaires, algèbre linéaire	255
8.1	Définition et notation	255
8.1.1	Opérations élémentaires sur les lignes ou colonnes	256
8.1.2	Transposition	257
8.1.3	Matrices particulières	257
8.2	Opérations	259
8.2.1	Addition	259
8.2.2	Multiplication d'une matrice par un élément de \mathbb{K}	259
8.2.3	Multiplication de deux matrices	260
8.3	Anneau des matrices carrées	263
8.3.1	Puissance d'une matrice carrée	263
8.3.2	Formule du binôme	263
8.3.3	Matrices carrées inversibles	263
8.4	Rang d'une matrice	265
8.4.1	Matrices ligne-équivalentes	265
8.4.2	L réduite échelonnée	266
8.4.3	Algorithme de Gauss-Jordan	268
8.5	Systèmes linéaires	272
8.5.1	Généralités	272
8.5.2	Systèmes équivalents et résolution	274
8.6	Les vecteurs de \mathbb{K}^n	279
8.6.1	Famille, combinaison linéaire	280
8.6.2	Sous espace vectoriel	281
8.6.3	Familles libres, liées, génératrices	282
8.6.4	Bases	283
8.6.5	Matrice d'une famille	286
8.6.6	Changement de base	291
8.6.7	Produit scalaire canonique	293
8.6.8	Sous espaces orthogonaux	294
8.7	Applications linéaires	296
8.7.1	Matrice d'une application linéaire	297
8.7.2	Image et contre image d'un <i>sev</i> , noyau	300
8.7.3	Applications linéaires et familles	301
8.8	Endomorphismes de \mathbb{K}^n	304
9	Codes correcteurs d'erreurs	307
9.1	Généralités	307
9.1.1	Distance de Hamming	309
9.1.2	Distance minimale	310
9.1.3	Code <i>t</i> -correcteur	312
9.2	Codes linéaires	313

9.2.1	Décodage, première technique	314
9.2.2	Décodage, deuxième technique	318
9.2.3	Décodage, troisième technique	319
9.2.4	Codes cycliques	321
9.2.5	Codes de Hamming binaires	330
9.2.6	Code de Golay, de Reed-Solomon	332

10 Arithmétique 333

10.1	Propriétés de \mathbb{N} et de \mathbb{Z}	333
10.2	Divisibilité dans \mathbb{Z}	334
10.2.1	Propriétés de la relation divise	334
10.2.2	Division euclidienne	335
10.3	PPCM	338
10.3.1	Ppcm de deux entiers	338
10.3.2	Ppcm de plusieurs entiers	339
10.4	PGCD	339
10.4.1	Propriétés immédiates	341
10.4.2	Algorithme d'Euclide	342
10.4.3	Algorithme d'Euclide étendu	345
10.4.4	Calcul du ppcm de deux entiers	351
10.5	Nombres premiers	352
10.6	Congruences	355
10.6.1	Propriétés	356
10.6.2	Congruences et opérations	358
10.6.3	Codes de contrôle	360
10.6.4	Exponentiation modulaire	361
10.7	Calculs modulo n	362
10.8	Fonction indicatrice d'Euler	370
10.9	Problèmes difficiles	375

11 Cryptographie civile 377

11.1	Terminologie	379
11.2	Difficulté calculatoire	381
11.3	Le code Vernam	383
11.4	Cryptosystèmes à clef secrètes	384
11.4.1	Le DES	384
11.4.2	Skip Jack	384
11.4.3	Rinjdael	384
11.5	Cryptosystèmes à clefs publiques	385
11.5.1	Le R.S.A.	385
11.5.2	El Gamal	387
11.6	Signatures numériques	388
11.7	Stockage de mots de passe	389
11.8	Authentification	390

A Raisonnement, récursion et induction 391

A.1	Le raisonnement	391
A.2	Principe de démonstration par récurrence	393

A.3	Induction	394
A.4	Système formel	396
B	Les logarithmes	397
B.1	La fonction logarithme népérien	397
B.2	Les fonctions logarithmes et exponentielles de base a	397
B.2.1	La fonction logarithme décimal ou de base 10	398
B.2.2	La fonction logarithme de base 2	398
B.2.3	Quelques utilisations	398
C	Dénombrément	401
C.1	Cardinaux	401
C.2	p -listes	403
C.3	p -listes d'éléments distincts	404
C.4	Combinaisons, nombre de parties	405
C.5	Combinaisons avec répétitions	407
C.6	Partages	408
C.7	Nombre de surjections	408
C.8	Nombre de partitions	410
C.9	Permutations, dérangements	412
D	Modélisation du hasard	415
D.1	Suites aléatoires	415
D.2	Simulation de variables aléatoires	416
E	Structures	417
E.1	Loi de composition interne (lci)	417
E.1.1	Propriétés et vocabulaire	417
E.2	Groupes	418
E.2.1	Soustraction	418
E.2.2	Sous groupe	419
E.2.3	Produit de groupes	419
E.2.4	Goupes finis	419
E.3	Anneaux	419
E.3.1	Éléments neutres d'un anneau	420
E.3.2	Diviseurs de zéro	420
E.3.3	Formule du binôme de Newton	420
E.3.4	Produit d'anneaux	421
E.3.5	Idéaux	421
E.4	Corps	421
E.5	Espace vectoriel	421
E.5.1	Espace vectoriel fondamental	421
E.6	Homomorphismes	422
E.7	Le corps fini à p éléments, p premier	422

E.7.1 Relation \equiv_n 422

E.7.2 Propriétés 423

E.7.3 Opérations 423

E.7.4 Pratique 424

E.7.5 Cas de \mathbb{F}_2 424