

Table des matières

Introduction	xiii
Pourquoi tant de théorie?	xiv
I Historique	1
1 Histoires d’algorithmes	3
1.1 La notion naïve d’algorithme	5
1.1.1 L’algorithme d’Euclide	7
1.1.2 Algorithme de l’équation quadratique	7
1.1.3 Un algorithme qui vient de loin	9
1.1.4 L’algorithme du Labyrinthe	11
II Survol	17
2 Un rapide tour d’horizon	19
2.1 Une stratégie de résolution	20
2.2 Deux exemples	20
2.3 Les classes \mathcal{P} et \mathcal{NP}	22
2.4 La classe \mathcal{NP}	22
2.4.1 Réductibilité polynomiale	23
2.4.2 La classe \mathcal{NPC}	24
2.5 Conclusion	25
3 La Machine de Turing	27
3.1 La Machine de Turing, modèle d’algorithme	27
3.1.1 Description d’une machine de Turing	29

3.1.2	Précision du concept d'algorithme	32
3.2	Un peu de formalisme	34
3.3	Machines de Turing élémentaires	35
3.3.1	Machine qui s'arrête	35
3.3.2	Machine "tout à gauche", machine "tout à droite"	35
3.3.3	Machine à effacement et écriture	36
3.3.4	Machines chercheuses de 1 ou de 0	36
3.3.5	Composition de machines	37
4	La Machine de Turing Universelle	39
4.1	Le problème général	39
4.1.1	Le problème du codage	41
4.1.2	Numérotation des Machines de Turing	46
4.2	Machine de Turing à plusieurs rubans	47
4.3	Calculateur, calculateur universel	49
4.3.1	Calculateur universel	51
4.3.2	Le nombre de Chaïtin	52
5	Complexité de Kolmogorov (<i>rudiments</i>)	53
5.1	Introduction	53
5.1.1	Interprétation intuitive	54
5.1.2	Paradoxe	54
5.2	Description d'un objet	55
5.2.1	Fonction partiellement récursive	56
5.3	Descriptions et tailles	57
III	Théorie	61
6	Considérations théoriques	63
6.1	Quelques définitions fondamentales	63
6.1.1	Le problème, informellement	63
6.1.2	Essais de définitions	64
6.1.3	Des ensembles bien particuliers	68
6.2	Indécidabilité	75
6.2.1	Plus ou moins indécidable	76
6.3	Mathématiques ou informatique ?	76

7	Ordres, Treillis et Algèbre de Boole	79
7.1	Relations d'équivalence	79
7.1.1	Ensemble quotient	79
7.2	Ordre, ordre partiel et préordre	80
7.2.1	Isomorphisme et dualité d'ensembles ordonnés	81
7.3	Treillis	82
7.3.1	Treillis distributifs	83
7.4	L'algèbre de Boole	84
7.5	L'algèbre de Boole des expressions logiques	84
7.6	Expressions booléennes et problème SAT	87
7.6.1	Satisfaction d'une expression	88
7.6.2	Algèbre de Boole	90
7.6.3	Le problème SAT	91
8	Circuits booléens	93
8.1	Portes et circuits digitaux	93
8.1.1	Base standard	95
8.2	Fonctions booléennes et circuits	98
8.3	Circuits booléens	99
9	Quelques problèmes de référence	103
9.1	Introduction à la théorie des graphes	103
9.1.1	Petit vocabulaire de théorie des graphes	104
9.1.2	Exemple de représentation de graphes	104
9.1.3	Sous-ensembles remarquables de sommets	106
9.1.4	Ensembles absorbants, nombre d'absorption	108
9.2	Existence de chemin	109
9.2.1	Complexité	113
9.3	Flot maximal	113
9.4	Couplage dans un graphe biparti	116
9.5	La satisfiabilité	118
9.5.1	Une technique algorithmique : <i>la réduction</i>	118
9.6	Le voyageur de commerce	120
10	Algorithme, résolution	125
10.1	Faire son choix	126
10.2	Pourquoi la complexité ?	127
10.3	Interpréter la complexité	130

10.4	Des mots	131
10.4.1	Problème, instance, solution	131
10.4.2	Algorithme	131
10.4.3	Taille d'une instance	132
10.5	Fonction de complexité en temps	132
10.6	Problèmes de décision, langages, codage	133
10.6.1	Problème de décision	133
10.6.2	Langage	134
10.6.3	Codage	135

IV Complexité 137

11 Modèles de calcul, classes de complexité 139

11.1	La Machine de Turing comme modèle de calcul	139
11.2	Langages et fonctions	142
11.3	Autres modèles de calcul	147
11.3.1	Automates de Markov	147
11.3.2	Machines RAM	148
11.3.3	Circuits booléens ou digitaux	149
11.3.4	Machine à plusieurs rubans	151
11.4	Complexité en temps	153
11.5	Complexité en espace	155
11.6	Relation entre les complexités	155
11.7	La classe \mathcal{P}	156
11.8	La classe \mathcal{NP}	157
11.8.1	Approche informelle de la classe \mathcal{NP}	158
11.8.2	Classe $\text{Co-}\mathcal{NP}$	160
11.9	La classe $\mathcal{NP} \cap \text{Co-}\mathcal{NP}$	162
11.9.1	Dualité	163

12 Complétude \mathcal{NP} 167

12.1	Le monde de \mathcal{NP}	167
12.1.1	La transformation polynomiale	167
12.2	La classe des problèmes \mathcal{NPC}	169
12.2.1	Un problème \mathcal{NP} – <i>complet</i>	171
12.2.2	Le problème SAT	171
12.3	SAT, problème \mathcal{NP} – <i>complet</i>	173

12.3.1	Le théorème de Lévine-Cook	174
12.3.2	Équilibre	183
12.3.3	L'appartenance à \mathcal{NPC}	184
12.3.4	Couverture d'un graphe	187
12.3.5	La classe $\text{Co-}\mathcal{NPC}$	191
12.3.6	Sur l'équivalence de certains problèmes	191
13	Le pire n'est pas toujours certain	197
13.1	Autour de SAT	197
13.1.1	Le cas 2-SAT	197
13.2	Cas particuliers de SAT	200
13.2.1	SET et SAT	200
13.2.2	Validation, tautologie et non-satisfiabilité	201
13.2.3	Clauses de Horn	202
13.3	Le sac à dos	205
13.3.1	Pseudo-polynomialité	208
13.4	Conclusion	209
14	Complexité et efficacité	211
14.1	Le produit matriciel	211
14.2	La multiplication de Straßen	213
14.3	Complexité de la méthode de Straßen	213
14.3.1	De la complexité à l'efficacité	215
14.3.2	La programmation récursive	216
14.4	Reformulation de la méthode de Straßen	217
14.4.1	Hypothèses et notations préliminaires	217
14.4.2	Proposition de Straßen	218
14.4.3	Généralisation	218
14.5	L'algorithme	220
14.5.1	Idée de base	220
14.5.2	Obtention des produits de Straßen	221
14.6	Règles d'obtention des termes	221
	Conclusion	221
V	Que faire ?	223
15	Des algorithmes pour problèmes \mathcal{NPC}	225

15.1	L'exhaustivité des procédures	225
15.1.1	La méthode PSEP	226
15.2	Le cas des jeux	230
15.2.1	La méthode alpha/bêta	232
15.3	En guise de conclusion	236
16	Introduction à l'algorithmique probabiliste	237
16.1	Des algorithmes aux parfums de casinos	237
16.1.1	Algorithmes numériques probabilistes	239
16.1.2	Algorithmes de Las Vegas	239
16.1.3	Algorithmes de Monte-Carlo	239
16.2	Probabilités <i>versus</i> déterminisme	240
16.2.1	Le problème	240
16.3	Les probabilités pour réduire la complexité	242
16.3.1	Généralités	242
16.3.2	Le Problème	242
16.3.3	L'algorithme de Borůkva	243
16.3.4	Arêtes "lourdes" et arbre couvrant	245
16.3.5	Échantillonnage aléatoire, arbre couvrant	246
16.3.6	Algorithme linéaire	248
16.3.7	Algorithme probabiliste d'arbre couvrant	248
16.4	Résoudre SAT de manière probabiliste	250
16.4.1	Rappel	250
16.4.2	2-SAT, solution probabiliste, analyse	251
16.4.3	Chaîne de Markov et complexité en temps	254
16.4.4	Généralisation à 3-SAT	256
16.4.5	Proposition d'algorithme modifié	259
16.5	Un problème d'accord	262
16.5.1	Un exemple issu de la Biologie	262
16.6	Une solution synchrone	263
16.6.1	Le protocole	264
16.6.2	Preuve de bon fonctionnement <i>in absurdo</i>	264
16.6.3	Évaluation de la complexité	265
16.7	Le cas asynchrone	265
16.7.1	Évaluation de la complexité	266
16.7.2	Preuve	267

17 De Shannon à Kolmogorov	269
17.1 L'entropie	270
17.1.1 L'information de Shannon	270
17.1.2 Généralisation	273
17.2 Notations	275
17.2.1 Le théorème d'invariance	277
17.2.2 Ne pas dépasser les bornes	281
17.2.3 Compressibilité et incompressibilité	282
18 Le modèle quantique	285
18.1 Introduction	285
18.2 Retour sur les bits classiques - Cbits	286
18.3 Opérations sur les Cbits	288
18.3.1 Transformation de Hadamard	292
18.4 Les bits quantiques ou Qbits	292
18.5 Opérations sur les Q-bits	294
18.6 Extraire l'information des Qbits?	296
A Notations de Bachman-Landau	299
A.1 Les symboles grand \mathcal{O} , Ω , Θ	299
A.1.1 Le symbole petit o	300
Index des noms cités	301
Index des noms cités	301
Index des concepts et notions	303
Index des concepts et notions	303
Index des algorithmes	310
Index des Algorithmes	310
Bibliographie	313