

informatique

méthodes

# Complexité et algorithmique avancée

*une introduction*

Ivan Lavallée



Hermann

*Ingénieur - Doctorat*

# Table des matières

<b>Remerciements</b>	<b>iii</b>
<b>Introduction</b>	<b>ix</b>
0.1 Pourquoi tant de théorie ? . . . . .	x
<b>I Historique</b>	<b>1</b>
<b>1 Histoires d'algorithmes</b>	<b>3</b>
1.1 La notion naïve d'algorithme . . . . .	4
1.1.1 L'algorithme d'Euclide . . . . .	6
1.1.2 Algorithme de l'équation quadratique . . . . .	7
1.1.3 Un algorithme qui vient de loin . . . . .	8
1.1.4 L'algorithme du Labyrinthe . . . . .	11
<b>II Survol</b>	<b>17</b>
<b>2 Un rapide tour d'horizon</b>	<b>19</b>
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

<b>3</b>	<b>La Machine de Turing</b>	<b>27</b>
3.1	La Machine de Turing, modèle d'algorithme . . . . .	27
3.1.1	Description détaillée 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" . . . . .	36
3.3.3	Machine à effacement et écriture . . . . .	36
3.3.4	Machines chercheuses de 1 ou de 0 . . . . .	37
3.3.5	Composition de machines de Turing élémentaires . . . . .	37
3.3.5.1	Mise en séquence de machines . . . . .	37
3.3.5.2	Branchement de machines . . . . .	38
<b>4</b>	<b>La Machine de Turing Universelle</b>	<b>39</b>
4.1	Le problème général . . . . .	39
4.1.1	Le problème du codage . . . . .	41
4.1.1.1	L'unidimensionnalité . . . . .	41
4.1.1.2	La finitude du codage . . . . .	42
4.1.1.3	Codage de l'instance . . . . .	44
4.1.2	Numérotation des Machines de Turing . . . . .	47
4.2	Machine de Turing à plusieurs rubans . . . . .	47
4.3	Calculateur, calculateur universel . . . . .	49
4.3.1	Calculateur universel . . . . .	52
4.3.2	Le nombre de Chaïtin . . . . .	52
<b>5</b>	<b>Complexité de Kolmogorov (<i>rudiments</i>)</b>	<b>55</b>
5.1	Introduction . . . . .	55
5.1.1	Interprétation intuitive . . . . .	56
5.1.2	Paradoxe . . . . .	57
5.2	Description d'un objet . . . . .	57
5.2.0.1	Fonction partiellement récursive . . . . .	58
5.3	Descriptions et tailles . . . . .	59

<b>III</b>	<b>Théorie</b>	<b>63</b>
<b>6</b>	<b>Considérations théoriques</b>	<b>65</b>
6.1	Quelques définitions fondamentales . . . . .	65
6.1.1	Le problème, informellement . . . . .	65
6.1.2	Essais de définitions . . . . .	66
6.1.2.1	Ensembles récursifs . . . . .	66
6.1.2.2	Ensemble récursivement énumérable .	67
6.1.2.3	Ensembles approximables et inapproxi- mables . . . . .	68
6.1.3	Des ensembles bien particuliers . . . . .	70
6.1.3.1	Taille d'un ensemble . . . . .	71
6.1.3.2	Des cardinaux à l'infini . . . . .	72
6.1.3.2.1	Cardinaux infinis . . . . .	73
6.1.3.2.2	Calcul sur les cardinaux in- finis . . . . .	74
6.1.3.2.3	Ensembles dénombrables . . . . .	75
6.1.3.2.4	De plus en plus infini . . . . .	76
6.2	Indécidabilité . . . . .	77
6.2.1	Plus ou moins indécidable . . . . .	79
6.3	Mathématiques ou informatique ? . . . . .	79
<b>7</b>	<b>Ordres, Treillis et Algèbre de Boole</b>	<b>81</b>
7.1	Relations d'équivalence . . . . .	81
7.1.1	Ensemble quotient . . . . .	81
7.2	Ordre, ordre partiel et préordre . . . . .	82
7.2.1	Isomorphisme et dualité d'ensembles ordonnés .	83
7.3	Treillis . . . . .	84
7.3.1	Treillis distributifs . . . . .	85
7.4	L'algèbre de Boole . . . . .	86
7.5	L'algèbre de Boole des expressions logiques . . . . .	86
7.6	Expressions booléennes et problème SAT . . . . .	88
7.6.1	Satisfaction d'une expression . . . . .	90
7.6.2	Algèbre de Boole . . . . .	92
7.6.2.1	Formes normales . . . . .	92
7.6.3	Le problème SAT . . . . .	93

<b>8</b>	<b>Circuits booléens</b>	<b>95</b>
8.1	Portes et circuits digitaux . . . . .	95
8.1.1	Base standard . . . . .	97
8.2	Fonctions booléennes et circuits . . . . .	100
8.3	Circuits booléens . . . . .	101
8.3.0.1	Circuit-SAT . . . . .	104
<b>9</b>	<b>Quelques problèmes de référence</b>	<b>105</b>
9.1	Introduction à la théorie des graphes . . . . .	105
9.1.1	Petit vocabulaire de théorie des graphes . . . . .	106
9.1.2	Exemple de représentation de graphes . . . . .	106
9.1.3	Quelques sous-ensembles remarquables de sommets . . . . .	108
9.1.4	Détermination des ensembles absorbants et du nombre d'absorption . . . . .	110
9.2	Existence de chemin . . . . .	111
9.2.1	Complexité . . . . .	115
9.3	Flot maximal . . . . .	116
9.4	Couplage dans un graphe biparti . . . . .	119
9.5	La satisfiabilité . . . . .	120
9.5.1	Une technique algorithmique : <i>la réduction</i> . . . . .	121
9.6	Le voyageur de commerce . . . . .	124
<b>10</b>	<b>Algorithme, résolution</b>	<b>129</b>
10.1	Faire son choix . . . . .	130
10.2	Pourquoi la complexité ? . . . . .	131
10.3	Comment interpréter la complexité ? . . . . .	135
10.4	Des mots . . . . .	135
10.4.1	Problème, instance, solution . . . . .	135
10.4.2	Algorithme . . . . .	136
10.4.3	Taille d'une instance . . . . .	136
10.5	Fonction de complexité en temps . . . . .	137
10.6	Problèmes de décision, langages, codage . . . . .	138
10.6.1	Problème de décision . . . . .	138
10.6.2	Langage . . . . .	139
10.6.3	Codage . . . . .	139

<b>IV</b>	<b>Complexité</b>	<b>143</b>
<b>11</b>	<b>Classes de complexité</b>	<b>145</b>
11.1	Machine de Turing et automates de Markov . . . . .	145
11.1.1	Automates de Markov . . . . .	150
11.1.1.1	Automate fini . . . . .	150
11.1.1.2	Langage accepté, régulier . . . . .	151
11.1.2	Machine à plusieurs rubans . . . . .	151
11.2	Langage reconnaissable par une MT . . . . .	153
11.2.1	Complexité en temps . . . . .	154
11.3	La classe $\mathcal{P}$ . . . . .	155
11.4	La classe $\mathcal{NP}$ . . . . .	156
11.4.1	Approche informelle de la classe $\mathcal{NP}$ . . . . .	156
<b>12</b>	<b><math>\mathcal{NP}</math> complétude</b>	<b>165</b>
12.1	Les relations entre $\mathcal{P}$ et $\mathcal{NP}$ . . . . .	165
12.1.1	La transformation polynomiale . . . . .	165
12.2	La classe des problèmes $\mathcal{NP}$ – <b>complets</b> , $\mathcal{NPC}$ . . . . .	167
12.2.1	Un problème $\mathcal{NP}$ – <i>complet</i> , la satisfiabilité . . . . .	169
12.2.2	Le problème de la satisfiabilité . . . . .	170
12.3	SAT, problème $\mathcal{NP}$ – <i>complet</i> . . . . .	171
12.3.1	Le théorème de Levin-Cook . . . . .	172
12.3.1.1	Première partie : SAT est dans $\mathcal{NP}$ . . . . .	172
12.3.1.2	Seconde partie . . . . .	172
12.3.2	Équilibre . . . . .	180
12.3.3	L'appartenance à $\mathcal{NPC}$ . . . . .	182
12.3.3.1	Le cas de k-SAT . . . . .	183
12.3.4	Couverture d'un graphe . . . . .	185
<b>13</b>	<b>Le pire n'est pas toujours certain</b>	<b>195</b>
13.1	Autour de SAT . . . . .	195
13.1.1	Le cas 2-SAT . . . . .	195
13.2	Cas particuliers de SAT . . . . .	198
13.2.1	SET et SAT . . . . .	198
13.2.2	Validation, tautologie et non-satisfiabilité . . . . .	199
13.2.3	Clauses de Horn . . . . .	200
13.3	Le sac à dos . . . . .	203

13.3.0.1	Recouvrement . . . . .	204
13.3.0.2	Retour à SAD . . . . .	205
13.3.1	Pseudo-polynomialité . . . . .	206
13.4	Conclusion . . . . .	207
<b>14</b>	<b>Complexité et Efficacité</b>	<b>209</b>
14.1	Le produit matriciel . . . . .	209
14.2	La multiplication de Straßen . . . . .	211
14.3	Complexité de la méthode de Straßen . . . . .	211
14.3.1	De la complexité à l'efficacité . . . . .	213
14.3.2	La programmation récursive . . . . .	214
14.4	Reformulation de la méthode de Straßen . . . . .	215
14.4.1	Hypothèses et notations préliminaires . . . . .	215
14.4.2	Proposition de Straßen . . . . .	216
14.4.3	Généralisation . . . . .	217
14.5	L'algorithme . . . . .	219
14.5.1	Idée de base . . . . .	219
14.5.2	Obtention des produits de Straßen . . . . .	219
14.6	Règles d'obtention des termes . . . . .	219
	Conclusion . . . . .	219
<b>V</b>	<b>Que faire ?</b>	<b>221</b>
<b>15</b>	<b>Des algorithmes pour problèmes <math>\mathcal{NPC}</math></b>	<b>223</b>
15.1	L'exhaustivité des procédures combinatoires . . . . .	223
15.1.1	La méthode PSEP . . . . .	224
15.1.1.1	Le principe de séparation . . . . .	224
15.1.1.2	L'évaluation . . . . .	225
15.1.1.2.1	La fonction d'évaluation : . . . . .	225
15.2	Le cas des jeux . . . . .	228
15.2.1	La méthode alpha/bêta . . . . .	231
15.3	En guise de conclusion . . . . .	234
<b>16</b>	<b>Introduction à l'algorithmique probabiliste</b>	<b>237</b>
16.1	Des algorithmes aux parfums de casinos . . . . .	237
16.1.0.0.2	Exemple . . . . .	238

16.1.1	Algorithmes numériques probabilistes . . . . .	239
16.1.2	Algorithmes de Las Vegas (deux cas à distinguer)	239
16.1.3	Algorithmes de Monte-Carlo . . . . .	240
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 Borükva . . . . .	244
16.3.3.1	Complexité de la phase Borükva . . . . .	245
16.3.4	Arêtes "lourdes" et vérification d'arbre couvrant minimum . . . . .	245
16.3.5	Echantillonnage aléatoire pour les arbres cou- vrants minimum . . . . .	247
16.3.6	Algorithme d'arbre couvrant minimum linéaire .	248
16.3.7	Algorithme probabiliste de construction d'un arbre couvrant minimal . . . . .	249
16.4	Résoudre SAT de manière probabiliste . . . . .	250
16.4.1	Rappel . . . . .	250
16.4.2	Analyse d'une solution probabiliste à 2-SAT . .	251
16.4.3	Etude de la chaîne de Markov permettant d'es- timer la complexité en temps de l'algorithme . .	254
16.4.3.1	Cas où la formule est éventuellement insatisfiable . . . . .	256
16.4.4	Généralisation à 3-SAT . . . . .	257
16.4.4.1	L'algorithme . . . . .	258
16.4.5	Proposition d'algorithme modifié . . . . .	260
16.5	Un problème d'accord . . . . .	263
16.5.1	Un exemple issu de la Biologie . . . . .	263
16.6	Une solution synchrone . . . . .	264
16.6.1	Le protocole . . . . .	265
16.6.2	Preuve de bon fonctionnement <i>in absurdo</i> . . . .	266
16.6.3	Évaluation de la complexité . . . . .	266
16.7	Le cas asynchrone . . . . .	266
16.7.1	Evaluation de la complexité . . . . .	268
16.7.2	Preuve . . . . .	268

<b>17</b>	<b>Kolmogorov le retour</b>	<b>271</b>
17.1	Introduction . . . . .	271
17.2	Information, codage, Shannon, Kolmogorov . . . . .	272
17.2.1	Entropie . . . . .	272
17.2.1.1	Le cas combinatoire . . . . .	272
17.2.1.2	Le cas probabiliste . . . . .	273
17.3	Notations . . . . .	277
17.3.1	Le théorème d'invariance . . . . .	279
17.3.2	Ne pas dépasser les bornes . . . . .	283
17.3.3	Compressibilité et incompressibilité . . . . .	284
<b>18</b>	<b>Le modèle quantique</b>	<b>287</b>
18.1	Introduction . . . . .	287
18.2	Retour sur les bits classiques - Cbits . . . . .	288
18.3	Opérations sur les Cbits . . . . .	290
18.3.1	Transformation de Hadamard . . . . .	294
18.4	Les bits quantiques ou Qbits . . . . .	294
18.5	Opérations sur les Q-bits . . . . .	296
18.6	Comment extraire l'information des Qbits ? . . . . .	298
<b>A</b>	<b>Notations de Bachman-Landau</b>	<b>301</b>
A.1	Les symboles grand $\mathcal{O}$ , $\Omega$ , $\Theta$ . . . . .	301
A.1.1	Le symbole petit $o$ . . . . .	302
	<b>Index</b>	<b>303</b>
	<b>Bibliographie</b>	<b>311</b>

# Table des figures

1.1	Une page du traité des 9 procédures . . . . .	5
1.2	Algorithme d'Al Khawarizmi . . . . .	7
1.3	Labyrinthe . . . . .	12
3.1	Machine de Turing . . . . .	31
6.1	Hiérarchie des ensembles . . . . .	70
8.1	Graphes de schémas logiques de circuits digitaux . . . . .	97
8.2	Schéma logique de circuit booléen . . . . .	99
8.3	Opérateurs booléens vs graphes . . . . .	102
8.4	Schématisation générale d'une expression booléenne . . . . .	103
9.1	Exemple de graphe . . . . .	107
9.2	Ensemble stable intérieurement . . . . .	108
9.3	Ensemble absorbant . . . . .	111
9.4	Existence de chemin entre deux sommets . . . . .	112
9.5	Exemple de graphe avec capacités . . . . .	118
9.6	Graphes bipartis avec et sans possibilité de couplage . . . . .	120
9.7	Couplage et flot . . . . .	121
9.8	Échecs et recouvrement . . . . .	123
9.9	Une instance du problème VRP . . . . .	126
12.1	Classes de complexité . . . . .	168
13.1	Interprétation graphique de 2-SAT . . . . .	197
15.1	Arborescence PSEP . . . . .	227

15.2	Arbre partiel du jeu de nim . . . . .	229
15.3	Arbre partiel du jeu de nim ré-évalué . . . . .	230
15.4	Arbre de jeu évalué pour alpha/béta . . . . .	231
15.5	Arbre de jeu et coupes alpha/béta . . . . .	234