

# Table des matières

<b>Introduction</b>	<b>ix</b>
<b>Préliminaires et notations</b>	<b>xv</b>
<b>1 Le modèle de calcul</b>	<b>1</b>
1.1 Problèmes, langages et codage	2
1.1.1 Codage	2
1.1.2 Problèmes et langages	3
1.2 La machine de Turing	5
1.2.1 Définition	5
1.2.2 Exemples	10
1.2.3 Code et machine universelle	14
1.2.4 Langage de haut niveau	27
1.2.5 Indécidabilité	29
<b>2 Considérations de base sur le temps</b>	<b>31</b>
2.1 Temps déterministe	31
2.1.1 Classes de complexité en temps	32
2.1.2 Théorème de hiérarchie	35
2.1.3 Temps polynomial et temps exponentiel	39
2.2 Temps non déterministe	43
2.2.1 Machines non déterministes	43
2.2.2 Langage de haut niveau	45
2.2.3 Machine non déterministe universelle	46
2.2.4 Classes en temps non déterministe	49
2.2.5 Théorème de hiérarchie en temps non déterministe	52

2.2.6	Temps non déterministe polynomial et exponentiel . . . . .	54
2.2.7	Le problème « $P = NP?$ » . . . . .	59
2.2.8	Complexité du complémentaire . . . . .	60
<b>3</b>	<b>NP-complétude</b> . . . . .	<b>63</b>
3.1	Réductions . . . . .	63
3.2	Complétude . . . . .	67
3.2.1	Définition et premières propriétés . . . . .	67
3.2.2	Complétude du problème SAT . . . . .	70
3.2.3	Autres problèmes NP-complets . . . . .	76
3.2.4	Complémentaire . . . . .	85
3.2.5	Théorème de Ladner . . . . .	86
3.2.6	Théorème de Mahaney . . . . .	90
3.2.7	Algorithme polynomial pour SAT si $P = NP$ . . . . .	93
<b>4</b>	<b>Considérations de base sur l'espace</b> . . . . .	<b>97</b>
4.1	Espace déterministe . . . . .	97
4.1.1	Définitions . . . . .	97
4.1.2	Espace logarithmique . . . . .	99
4.1.3	Composition . . . . .	101
4.1.4	Théorème de hiérarchie . . . . .	102
4.2	Espace non déterministe . . . . .	103
4.3	Comparaison avec les classes en temps . . . . .	104
4.4	Complétude . . . . .	110
4.4.1	Espace polynomial . . . . .	110
4.4.2	Espace non déterministe logarithmique . . . . .	112
4.5	Le rôle du non-déterminisme . . . . .	116
4.5.1	Certificats unidirectionnels . . . . .	116
4.5.2	Théorème de Savitch . . . . .	118
4.5.3	Théorème d'Immerman-Szelepcsényi . . . . .	120
4.5.4	Les questions ouvertes . . . . .	126
<b>5</b>	<b>Uniformité et non-uniformité</b> . . . . .	<b>127</b>
5.1	Conseils . . . . .	128
5.1.1	Définition . . . . .	128

---

5.1.2	Classes usuelles . . . . .	129
5.1.3	Premiers résultats . . . . .	131
5.2	Circuits booléens . . . . .	133
5.2.1	Définition . . . . .	133
5.2.2	Machines et circuits . . . . .	137
5.2.3	Circuits et conseils . . . . .	141
5.3	Uniformité des circuits . . . . .	142
5.4	Autres classes définies par circuits . . . . .	143
5.5	Intérêt des circuits et bornes inférieures non uniformes . . . . .	145
5.6	Circuits arithmétiques . . . . .	146
<b>6</b>	<b>Algorithmes probabilistes</b> . . . . .	<b>153</b>
6.1	Machines de Turing probabilistes . . . . .	153
6.1.1	Tri rapide . . . . .	153
6.1.2	Machines de Turing probabilistes . . . . .	155
6.2	Classes probabilistes . . . . .	155
6.2.1	Définitions . . . . .	156
6.2.2	Réduction d'erreur . . . . .	157
6.2.3	Comparaison avec les classes uniformes . . . . .	159
6.2.4	Théorème de hiérarchie . . . . .	160
6.2.5	Circuits et algorithmes probabilistes . . . . .	163
6.3	Un exemple important . . . . .	163
6.3.1	Test de circuits arithmétiques . . . . .	163
6.3.2	Équivalence des deux problèmes . . . . .	164
6.3.3	Algorithme probabiliste . . . . .	166
6.4	Questions ouvertes . . . . .	167
6.4.1	Problèmes naturels de BPP . . . . .	167
6.4.2	Hiérarchie . . . . .	167
6.4.3	Temps exponentiel . . . . .	168
<b>7</b>	<b>Oracles et limites de la diagonalisation</b> . . . . .	<b>169</b>
7.1	Théorèmes de hiérarchie . . . . .	169
7.1.1	Énumération des machines . . . . .	170
7.1.2	Hiérarchie déterministe . . . . .	170
7.2	Machines de Turing à oracle . . . . .	173

7.3	Quelques résultats pour se faire la main . . . . .	176
7.4	Langages creux et réduction Turing . . . . .	180
7.4.1	Langages creux . . . . .	180
7.4.2	Réduction Turing polynomiale . . . . .	182
7.5	Relativisation . . . . .	183
7.5.1	Diagonalisation, oracles et la question « $P = NP?$ » . . . . .	183
7.5.2	Relativisation de la question « $EXP = NP?$ » . . . . .	186
7.6	De la difficulté de définir la bonne notion de diagonalisation . . . . .	190
<b>8</b>	<b>La hiérarchie polynomiale</b>	<b>193</b>
8.1	La hiérarchie polynomiale . . . . .	193
8.1.1	Définition et premières propriétés . . . . .	193
8.1.2	Caractérisation en termes de quantificateurs . . . . .	196
8.1.3	Problèmes complets . . . . .	199
8.2	Comparaison avec les classes probabilistes . . . . .	201
8.3	Liens avec les circuits . . . . .	204
8.3.1	Théorème de Karp et Lipton . . . . .	204
8.3.2	Langages creux . . . . .	206
8.4	Borne inférieure sur le temps et l'espace conjugués pour $NTIME(n)$ . . . .	207
<b>9</b>	<b>Comptage</b>	<b>211</b>
9.1	Définitions . . . . .	211
9.1.1	Classes de fonctions . . . . .	212
9.1.2	Classes de langages . . . . .	214
9.2	Premiers résultats de complétude . . . . .	216
9.2.1	Réductions pour les classes de fonctions . . . . .	217
9.2.2	Complétude pour $\#P$ . . . . .	218
9.2.3	Complétude pour les autres classes . . . . .	219
9.3	Propriétés de clôture . . . . .	221
9.3.1	Propriétés de base . . . . .	221
9.3.2	$PP$ est clos par union . . . . .	223
9.3.3	$\#P$ est-il clos par soustraction? . . . . .	225
9.4	Théorème de Toda . . . . .	226
9.5	Permanent . . . . .	235
9.5.1	Intérêts du permanent . . . . .	236

9.5.2	Complétude du permanent	238
<b>10</b>	<b>Protocoles interactifs</b>	<b>247</b>
10.1	Les classes IP	248
10.1.1	Définition	248
10.1.2	Isomorphisme de graphes	250
10.1.3	$IP = PSPACE$	252
10.2	Les classes Arthur-Merlin	264
10.2.1	Définitions	265
10.2.2	Deux petits tours et puis s'en vont	267
10.2.3	Erreur d'un seul côté	269
10.2.4	Bits aléatoires publics ou privés	272
10.2.5	Le problème de l'isomorphisme de graphes	280
10.3	Le théorème PCP	281
10.3.1	Probabilistically Checkable Proofs	281
10.3.2	Résultats	283
<b>11</b>	<b>Bornes inférieures non uniformes</b>	<b>287</b>
11.1	Circuits booléens sans restriction	287
11.1.1	Bornes inférieures en $\Omega(n^k)$	288
11.1.2	Bornes inférieures en $n^{\omega(1)}$	292
11.2	Circuits restreints	296
11.2.1	Monotonie	297
11.2.2	Profondeur constante	298
11.3	Polynômes	304
11.3.1	Baur et Strassen	305
11.3.2	Borne inférieure en $\Omega(n^k)$	311
<b>12</b>	<b>Dérandomisation et bornes inférieures</b>	<b>317</b>
12.1	Dérandomisation	318
12.2	Imprédictibilité implique dérandomisation	320
12.3	Difficulté en moyenne implique imprédictibilité	324
12.4	Difficulté dans le pire cas implique difficulté en moyenne	330
12.4.1	Codes correcteurs d'erreurs	330
12.4.2	Application	347

12.5 Dérandomisation implique borne inférieure . . . . .	350
<b>A Probabilités et arithmétique</b>	<b>355</b>
A.1 Probabilités . . . . .	355
A.2 Arithmétique . . . . .	361
<b>B Exercices supplémentaires</b>	<b>363</b>
<b>C Solutions des exercices</b>	<b>369</b>
<b>D Classes de complexité rencontrées dans ce livre</b>	<b>389</b>
<b>E Indications pour l'enseignant</b>	<b>395</b>
<b>Bibliographie</b>	<b>399</b>
<b>Index</b>	<b>407</b>