

Table des matières

1	Rappels d'algèbre linéaire	1
1.1	Quelques propriétés générales	1
1.1.1	Notations	1
1.1.2	Formule de Binet-Cauchy	4
1.1.3	Rang, déterminant et identités de Cramer	5
1.1.4	Identités de Sylvester	9
1.2	Polynôme caractéristique	11
1.2.1	Matrice caractéristique adjointe	11
1.2.2	Formule de Samuelson	13
1.2.3	Valeurs propres de $f(A)$	14
1.3	Polynôme minimal	17
1.3.1	Sous-espaces de Krylov	17
1.3.2	Cas de matrices à coefficients dans \mathbb{Z}	20
1.4	Suites récurrentes linéaires	21
1.4.1	Polynôme générateur, opérateur de décalage	21
1.4.2	Matrices de Hankel	23
1.5	Polynômes symétriques et relations de Newton	25
1.6	Inégalité de Hadamard et calcul modulaire	30
1.6.1	Normes matricielles	30
1.6.2	Théorème chinois et applications	31
1.7	Résolution uniforme des systèmes linéaires	33
1.7.1	L'inverse de Moore-Penrose	34
1.7.2	Généralisation sur un corps arbitraire	41
2	Algorithmes de base en algèbre linéaire	51
2.1	Méthode du pivot de Gauss	53
2.1.1	Transformations élémentaires	53
2.1.2	La LU -décomposition	56
2.1.3	Recherche de pivot non nul	61

2.2	Méthode de Jordan-Bareiss	65
2.2.1	Formule de Dodgson-Jordan-Bareiss	66
2.2.2	Méthode de Jordan-Bareiss modifiée	70
2.2.3	La méthode de Dodgson	71
2.3	Méthode de Hessenberg	74
2.4	Méthode d'interpolation de Lagrange	81
2.5	Méthode de Le Verrier et variantes	82
2.5.1	Le principe général	82
2.5.2	Méthode de Souriau-Faddeev-Frame	83
2.5.3	Méthode de Preparata & Sarwate	88
2.6	Méthode de Samuelson-Berkowitz	90
2.6.1	Principe général de l'algorithme	90
2.6.2	Version séquentielle	91
2.7	Méthode de Chistov	93
2.7.1	Le principe général	93
2.7.2	La version séquentielle	95
2.8	Méthodes reliées aux suites récurrentes linéaires	97
2.8.1	L'algorithme de Frobenius	98
2.8.2	Algorithme de Berlekamp/Massey	108
2.8.3	Méthode de Wiedemann	109

3 Circuits arithmétiques **111**

3.1	Circuits arithmétiques et programmes d'évaluation	112
3.1.1	Quelques définitions	112
3.1.2	Circuit arithmétique vu comme un graphe	116
3.1.3	Circuits arithmétiques homogènes	118
3.1.4	Le problème des divisions	119
3.2	Élimination des divisions à la Strassen	120
3.2.1	Le principe général	121
3.2.2	Coût de l'élimination des divisions	125
3.3	Calcul des dérivées partielles	126

4 Notions de complexité **129**

4.1	Machines de Turing et Machines à Accès Direct	129
4.2	Complexité binaire, les classes \mathcal{P} , \mathcal{NP} et $\#\mathcal{P}$	134
4.2.1	Calculs faisables	134
4.2.2	Quand les solutions sont faciles à tester	135
4.2.3	Problèmes de comptage	141
4.3	Complexités arithmétique et binaire	142
4.3.1	Complexité arithmétique	142

4.3.2	Complexité binaire	143
4.4	Familles uniformes de circuits	149
4.5	Machines parallèles à accès direct	151
4.5.1	Une idéalisation des calculs parallèles	152
4.5.2	PRAM-complexité et Processeur-efficacité	153
4.5.3	Le principe de Brent	156
5	Diviser pour gagner	159
5.1	Le principe général	159
5.2	Circuit binaire équilibré	162
5.3	Calcul parallèle des préfixes	163
6	Multiplication rapide des polynômes	171
6.1	Méthode de Karatsuba	172
6.2	Transformation de Fourier discrète usuelle	175
6.3	Transformation de Fourier discrète rapide	177
6.3.1	Cas favorable	177
6.3.2	Cas d'un anneau commutatif arbitraire	180
6.4	Produits de matrices de Toeplitz	182
7	Multiplication rapide des matrices	185
7.1	Analyse de la méthode de Strassen	187
7.1.1	La méthode et sa complexité	187
7.1.2	Une famille uniforme de circuits arithmétiques	191
7.2	Inversion des matrices triangulaires	195
7.3	Complexité bilinéaire	197
7.3.1	Rang tensoriel d'une application bilinéaire	198
7.3.2	Exposant de la multiplication des matrices carrées	204
7.3.3	Complexités bilinéaire et multiplicative	205
7.3.4	Extension du corps de base	207
7.4	Calculs bilinéaires approximatifs	209
7.4.1	Méthode de Bini	209
7.4.2	Une amélioration décisive de Schönhage	214
7.4.3	Sommes directes d'applications bilinéaires	221
7.4.4	L'inégalité asymptotique de Schönhage	224
8	Algèbre linéaire séquentielle rapide	229
8.1	L'Algorithme de Bunch & Hopcroft	231
8.2	Calcul du déterminant et de l'inverse	235
8.3	Forme réduite échelonnée en lignes	236

8.4	Méthode de Keller-Gehrig	243
8.5	Méthode de Kaltofen-Wiedemann	245
9	Parallélisations de la méthode de Leverrier	255
9.1	Algorithme de Csanky	255
9.2	Amélioration de Preparata et Sarwate	259
9.3	Amélioration de Galil et Pan	266
10	Polynôme caractéristique sur un anneau arbitraire	271
10.1	Méthode générale de parallélisation	271
10.2	Algorithme de Berkowitz amélioré	272
10.3	Méthode de Chistov	283
10.4	Applications des algorithmes	287
11	Résultats expérimentaux	291
11.1	Tableaux récapitulatifs des complexités	291
11.2	Présentation des tests	295
11.3	Tableaux de Comparaison	296
12	Le déterminant et les expressions arithmétiques	303
12.1	Expressions, circuits et descriptions	303
12.2	Parallélisation des expressions et des circuits	309
12.3	La plupart des polynômes sont difficiles à évaluer	313
12.4	Le caractère universel du déterminant	315
13	Le permanent et la conjecture $\mathcal{P} \neq \mathcal{NP}$	321
13.1	Familles d'expressions et de circuits booléens	321
13.2	Booléen versus algébrique	328
13.2.1	Évaluation booléenne des circuits arithmétiques	328
13.2.2	Simulation algébrique des circuits et expressions booléennes	330
13.2.3	Formes algébriques déployées	333
13.3	Complexité binaire versus complexité booléenne	335
13.4	Le caractère universel du permanent	339
13.5	La conjecture de Valiant	340

Tables, bibliographie, index.

355

Liste des algorithmes, circuits et programmes d'évaluation . . .	355
Liste des Figures	357
Bibliographie	359
Index des notations	371
Index des termes	373