

**INFORMATIQUE
ET SYSTÈMES
D'INFORMATION**

Information - Commande - Communication

Calcul et arithmétique des ordinateurs

sous la direction de
Jean-Claude Bajard
Jean-Michel Muller

hermes

Lavoisier

Le traité Information, Commande, Communication répond au besoin de disposer d'un ensemble complet des connaissances et méthodes nécessaires à la maîtrise des systèmes technologiques.

Conçu volontairement dans un esprit d'échange disciplinaire, le traité IC2 est l'état de l'art dans les domaines suivants retenus par le comité scientifique :

- Réseaux et télécoms
- Traitement du signal et de l'image
- Informatique et systèmes d'information
- Systèmes automatisés et productique
- Management et gestion des STICS
- Cognition et traitement de l'information.

Chaque ouvrage présente aussi bien les aspects fondamentaux qu'expérimentaux. Une classification des différents articles contenus dans chacun, une bibliographie et un index détaillé orientent le lecteur vers ses points d'intérêt immédiats : celui-ci dispose ainsi d'un guide pour ses réflexions ou pour ses choix.

Les savoirs, théories et méthodes rassemblés dans chaque ouvrage ont été choisis pour leur pertinence dans l'avancée des connaissances ou pour la qualité des résultats obtenus dans le cas d'expérimentations réelles.



Table des matières

Introduction	15
0.1. Bibliographie	20
PREMIÈRE PARTIE. REPRÉSENTATION EN MACHINE ET ÉVALUATION ..	23
Chapitre 1. Représentation des nombres	25
Marc Daumas et Jean-Michel Muller	
1.1. Introduction	25
1.2. Représentation de position des entiers	25
1.2.1. Représentation « de position » des entiers positifs	25
1.2.2. Représentation de position des entiers signés	29
1.2.2.1. Représentation par signe et valeur absolue	29
1.2.2.2. Représentation en complément à la base	29
1.2.2.3. Représentations biaisées des entiers signés	32
1.2.3. Représentations redondantes	32
1.2.3.1. Représentations d'Avizienis	33
1.2.3.2. Représentations « carry save » et « borrow save »	34
1.2.4. Représentations modulaires des entiers	37
1.3. La représentation virgule flottante	39
1.3.1. Quelques généralités	39
1.3.2. Les modes d'arrondi	41
1.3.3. Les formats spécifiés par la norme IEEE-754	43
1.3.4. Les exceptions et leur traitement	45
1.3.4.1. Valeurs infinies et nombres dénormalisés	45
1.3.4.2. Quantités Not a Number	49
1.3.4.3. Tests portant sur des NaN	50
1.3.4.4. Codage des valeurs particulières	50
1.3.5. Conversions	51
1.3.6. La multiplication-accumulation	52

10. Calcul et arithmétique des ordinateurs

1.3.7. Tester son environnement virgule flottante	53
1.3.8. Quelques lectures	54
1.4. Bibliographie	54
Chapitre 2. Méthodes générales d'addition et multiplication	59
Jean-Michel Muller	
2.1. Introduction	59
2.2. L'addition en binaire : généralités	60
2.3. Le principe d'addition avec retenue conditionnelle	61
2.4. Le théorème de Winograd	62
2.5. Les fonctions magiques : <i>Generate</i> et <i>Propagate</i>	64
2.6. Les additionneurs à retenue anticipée	66
2.7. Les additionneurs <i>parallel prefix</i>	66
2.8. D'autres solutions	70
2.9. La multiplication	72
2.10. Multiplication par réseau cellulaire	72
2.11. Décomposition récursive de la multiplication	73
2.12. Multiplication arborescente en temps logarithmique	74
2.13. Le recodage de Booth	76
2.14. Bibliographie	79
Chapitre 3. Evaluation des Fonctions élémentaires	83
Jean-Michel Muller	
3.1. Introduction	83
3.2. La réduction d'argument	86
3.3. Mettre au point des approximations polynomiales	88
3.3.1. Obtenir de «bonnes» approximations	88
3.4. Un exemple : le calcul de l'exponentielle	93
3.4.1. Réduction d'argument	94
3.4.2. Approximation choisie	94
3.5. Le dilemme du fabricant de tables	98
3.6. L'algorithme CORDIC	101
3.6.1. Une méthode simple pour peser du pain	101
3.6.2. De la pesée du pain vers l'évaluation des fonctions trigonométriques	102
3.6.3. L'algorithme CORDIC généralisé	103
3.7. Conclusion	105
3.8. Bibliographie	105
Chapitre 4. Opérateurs sur circuits FPGA	109
Arnaud Tisserand et Jean-Luc Beuchat	
4.1. Introduction	109
4.2. Circuits FPGA	109

4.2.1. Architecture générale des FPGA	112
4.2.2. Exemples de circuits actuels : les familles Virtex et Spartan de Xilinx	115
4.3. Opérations de base	118
4.3.1. Addition	118
4.3.1.1. Additionneurs séquentiels rapides sur FPGA	119
4.3.2. Multiplication	120
4.3.3. Génération des produits partiels	121
4.3.4. Réduction des produits partiels	122
4.3.5. Addition finale	123
4.3.6. Multiplication/addition fusionnée	123
4.3.7. Carré	124
4.3.8. Petits blocs de multiplication câblée	124
4.4. Fonctions algébriques et élémentaires	125
4.4.1. Division	126
4.4.2. Racine carrée	129
4.4.3. Évaluation des fonctions élémentaires sur FPGA	129
4.4.4. Évaluation de polynômes sur FPGAs	129
4.4.5. Algorithmes à base d'additions et de décalages	130
4.4.6. Méthodes à base de tables et d'additions	130
4.5. Arithmétique sérielle	131
4.5.1. Modes de transmission des données	132
4.5.2. Arithmétique sérielle classique	134
4.5.2.1. Addition et soustraction sérielles	134
4.5.2.2. Multiplication et élévation au carré sérielles	135
4.5.2.3. Multiplication parallèle-série	137
4.5.3. Arithmétique en-ligne	139
4.5.3.1. Opérations de base et fonctions algébriques	139
4.5.3.2. Évaluation en-ligne de fonctions élémentaires	141
4.6. Arithmétique modulaire sur FPGA	142
4.6.1. Addition modulaire	143
4.6.2. Multiplication modulaire	145
4.6.2.1. Opérateurs parallèles	145
4.6.2.2. Opérateurs parallèle-série	148
4.7. Bibliographie	150
DEUXIÈME PARTIE. EXTENSIONS	153
Chapitre 5. Arithmétique multiprécision	155
Laurent Imbert	
5.1. Introduction	155
5.2. Comment représenter un grand nombre ?	156
5.2.1. Représentation des entiers	156

5.2.2. Représentation des nombres réels	157
5.3. Opérations arithmétiques élémentaires sur les grands entiers	158
5.3.1. La normalisation	158
5.3.2. L'addition et la soustraction	158
5.3.3. La multiplication par un petit entier	159
5.3.4. La division par un petit entier	159
5.3.5. La multiplication de deux grands entiers par l'algorithme usuel	159
5.4. Comment multiplier plus rapidement?	160
5.4.1. Les méthodes de Knuth, Karatsuba et Toom-Cook	160
5.4.2. La méthode de Schönhage et Strassen	164
5.4.2.1. La transformée de Fourier discrète	165
5.4.2.2. L'algorithme FFT	166
5.4.2.3. Application à la multiplication de grands entiers	166
5.4.2.4. Implantation	167
5.5. Division et racine carrée	168
5.5.1. La méthode de Newton-Raphson	168
5.5.2. La méthode de Goldschmidt	169
5.6. Fonctions élémentaires	170
5.6.1. Les approximations polynomiales	170
5.6.2. La moyenne arithmético-géométrique de Gauss-Legendre	173
5.6.3. La « Binary Splitting Method »	175
5.6.4. Quelques mots sur des méthodes mixtes	175
5.7. Ressources	176
5.8. Bibliographie	177

Chapitre 6. Systèmes modulaires de représentation

Laurent-Stéphane Didier

6.1. Introduction	181
6.2. Les principes de la représentation modulaire	182
6.2.1. Les systèmes modulaires de représentation (Residue Number Systems)	182
6.2.2. Opérations de base	185
6.2.3. Conversions	186
6.2.3.1. Conversion des systèmes de numération de position vers les systèmes modulaires	187
6.2.3.2. Conversion des systèmes modulaires vers les systèmes de numération de position	187
6.3. Diverses applications de la conversion	191
6.3.1. Extension et changement de base	191
6.3.1.1. Extension de base de Szabo et Tanaka	192
6.3.1.2. Extension de base de Shenoy et Kumaresan	192
6.3.2. Comparaison	193
6.3.2.1. Comparaison par changement de base	193

6.3.2.2. Comparaison de Chiang et Lu	193
6.3.2.3. Comparaison de Dimauro, Impedovo et Pirlo	194
6.4. Autres opérations dans les systèmes modulaires	194
6.4.1. Division	195
6.4.1.1. Cas particulier de la division exacte (sans reste)	195
6.4.1.2. Division de Gamberger	196
6.4.2. Multiplication modulaire dans un système modulaire	197
6.5. Conclusion	201
6.6. Bibliographie	201
Chapitre 7. Calcul sur les corps finis	207
Jean-Claude Bajard	
7.1. Des généralités	208
7.2. La multiplication dans $GF(2^m)$	209
7.2.1. Algorithme de Montgomery	210
7.2.1.1. Présentation de l'algorithme original	210
7.2.1.2. Algorithme de Montgomery sur les corps finis	211
7.2.1.3. Version itérative	213
7.2.2. Méthode de Mastrovito	214
7.2.3. Utilisation d'une base normale	216
7.2.4. Bases duales	219
7.3. La division	222
7.3.1. Utilisation de l'algorithme d'Euclide	222
7.3.2. Utilisation du petit théorème de Fermat	224
7.4. Perspectives	225
7.5. Bibliographie	225