

Table des matières

Note des traducteurs	v
Introduction à l'informatique quantique	vii
Préface	xiii
Commentaire sur les références bibliographiques	xvii
1 Les Cbits et les Qbits	1
1.1 Qu'est-ce qu'un ordinateur quantique?	1
1.2 Les Cbits et leurs états	3
1.3 Opérations réversibles sur les Cbits	8
1.4 Opérations de manipulation des Cbits	12
1.5 Les Qbits et leurs états	18
1.6 Opérations réversibles sur les Qbits	20
1.7 Diagrammes de circuits équivalents	22
1.8 Opérateur de mesure et la règle de Born	24
1.9 La règle de Born généralisée	30
1.10 Le rôle des portes de mesure dans la préparation d'un état	32
1.11 Construction d'états arbitraires à 1- ou 2-Qbits	34
1.12 Résumé : les Qbits et les Cbits	36
2 Généralités sur le calcul quantique et quelques exemples simples	39
2.1 Généralités sur le calcul quantique	39
2.2 Le problème de David Deutsch	44
2.3 Pourquoi les Qbits additionnels ne sèment pas forcément la pagaille	50
2.4 Le problème de Bernstein-Vazirani	54
2.5 Le problème de Simon	59
2.6 La construction des portes de Toffoli	64

3	Casser le cryptage RSA	71
3.1	Calcul de la période d'une fonction, factorisation d'un nombre et cryptographie	71
3.2	Préliminaires sur la théorie des nombres	73
3.3	Le cryptage RSA	75
3.4	Algorithme quantique de détermination de la période : remarques préliminaires	78
3.5	La transformée de Fourier quantique	80
3.6	Comment s'affranchir des portes à 2-Qbits	85
3.7	Comment trouver la période d'une fonction	89
3.8	Le calcul de la fonction périodique	93
3.9	L'insensibilité aux petites erreurs de phase	95
3.10	Relation entre la détermination de la période et la factorisation	97
4	Chercher avec un ordinateur quantique	99
4.1	Quel type de recherche ?	99
4.2	L'itération de Grover	100
4.3	Comment construire l'opérateur W	106
4.4	Généralisation à la recherche de plusieurs nombres spéciaux	108
4.5	Chercher un élément parmi quatre	111
5	La correction d'erreurs quantiques	113
5.1	Le miracle de la correction d'erreurs quantiques	113
5.2	Un exemple simplifié	115
5.3	La physique cachée derrière l'apparition des erreurs	124
5.4	Diagnostiquer les syndromes d'erreurs	129
5.5	Le code de correction d'erreurs à 5-Qbits	133
5.6	Le code de correction d'erreurs à 7-Qbits	137
5.7	Quelques opérations sur les séquences d'encodage à 7-Qbits	141
5.8	Un circuit d'encodage à 7-Qbits	143
5.9	Un circuit d'encodage à 5-Qbits	145
6	Quelques protocoles qui n'utilisent qu'un nombre restreint de Qbits	153
6.1	Les états de Bell	153
6.2	La cryptographie quantique	155
6.3	Mise en gage d'un bit	161
6.4	Le codage super-dense	164
6.5	La téléportation quantique d'état	168
6.6	L'étrange histoire des états GHZ	172

Annexe A : Espaces vectoriels complexes : propriétés élémentaires et notation de Dirac	179
Annexe B : Structure générale des transformations unitaires à 1-Qbit	189
Annexe C : Structure générale des états à 1-Qbit	195
Annexe D : Une action à distance mystérieuse	197
Annexe E : La cohérence de la règle de Born généralisée	205
Annexe F : D'autres aspects du problème de David Deutsch	207
Annexe G : La probabilité de succès pour le problème de Simon	211
Annexe H : Une façon de fabriquer une porte cNOT	215
Annexe I : Quelques notions élémentaires de théorie des groupes	219
Annexe J : Quelques notions élémentaires de théorie des nombres	221
Annexe K : Fractions continues et détermination de la période d'une fonction	223
Annexe L : Une estimation plus juste des chances de détermination de la période d'une fonction	227
Annexe M : La factorisation et la détermination de la période d'une fonction	229
Annexe N : Le code de correction d'erreurs à 9-Qbits de Shor	233
Annexe O : Traitement du code de correction d'erreurs à 7-Qbits par l'approche des diagrammes des circuits équivalents	237
Annexe P : À propos de la mise en gage d'un bit	245
Index	247