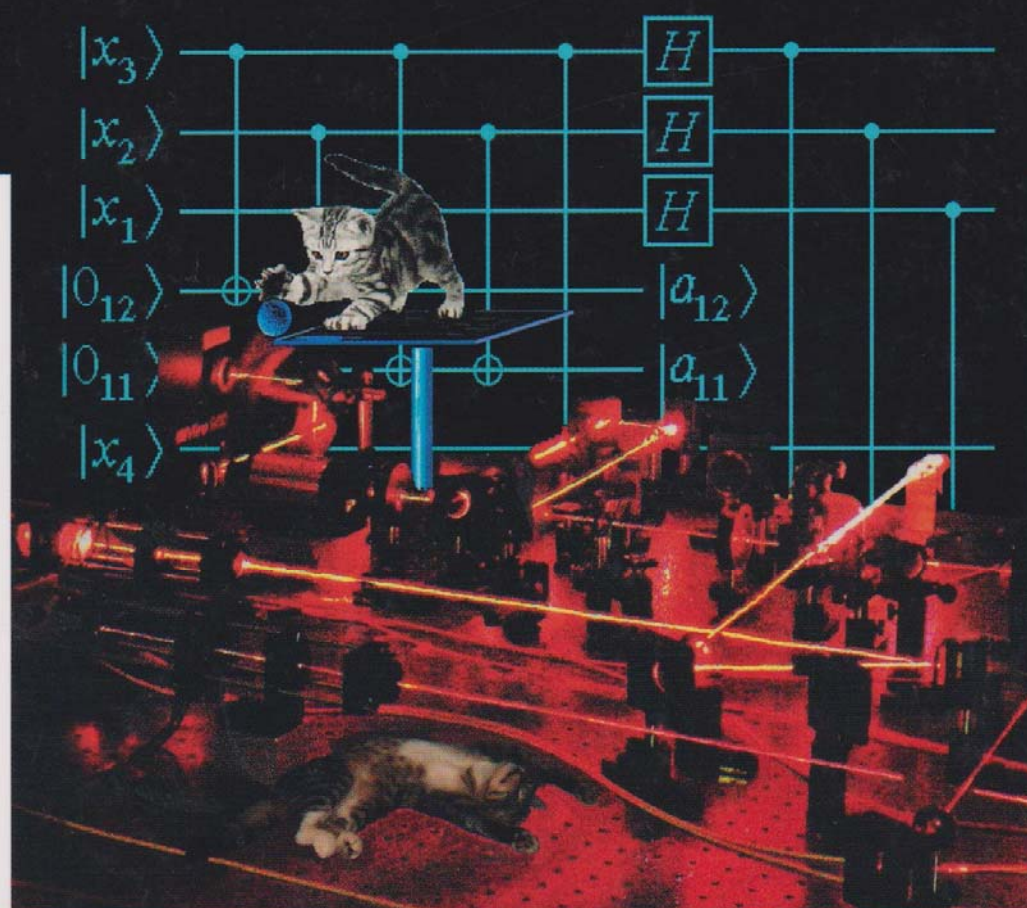
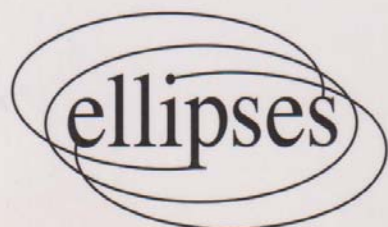


Charles Corge

L'informatique quantique



qu'est-ce et pour quoi faire ?



2-005-809-1

L'informatique quantique, qu'est-ce et pour quoi faire ?

Charles CORGE

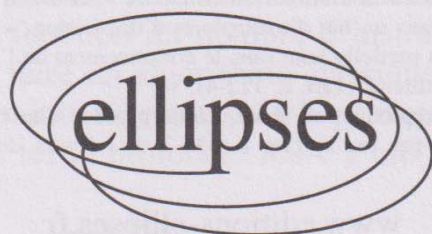


TABLE DES MATIÈRES

AVANT-PROPOS

III

CHAPITRE I

Les quanta s'invitent

I-1. L'Univers est en constante évolution	2
I-2. L'âge de l'Univers	4
I-2.1. Le rayonnement fossile témoigne	4
I-2.2. Les amas globulaires et les quasars confirment	7
I-2.3. La radioactivité contresigne	8
I-3. Sur les premières marches de la « Schola Quantorum »	9
I-3.1. L'effet photoélectrique	12
I-3.2. L'effet Compton	12
I-3.3. La diffraction des électrons et la dualité onde-corpuscule	13
I-4. Quantification de l'espace	16
I-4.1. Les quanta sont nichés au sein de l'atome	16
I-4.2. Le spin de l'électron	18
I-4.3. La polarisation de la lumière et la notion d'amplitude de probabilité	19
I-5. En bref	28

CHAPITRE II

Schola Quantorum : 1^{re} année Le cadre mathématique

II-1. Vecteurs et opérateurs	31
II-1.1. Espace vectoriel et vecteurs kets	31
II-1.2. Espace vectoriel dual et vecteurs bras	33
II-1.3. Produit scalaire	34
II-1.4. Espace de Hilbert	36
II-1.5. Opérateurs linéaires	36
II-1.6. Produit tensoriel	38
II-2. Opérateurs hermitiques, projecteurs et observables	40
II-2.1. Opérateurs adjoints, hermitiques, unitaires	40
II-2.2. Valeurs propres, vecteurs propres et observables	41
II-2.3. Projecteurs et leur algèbre	43
II-2.4. Spectre d'une observable et diagonalisation	45
II-2.5. Fonction d'observable	46
II-3. Théorie de la représentation	48
II-3.1. Représentation matricielle des vecteurs et opérateurs	48
II-3.2. Matrices de Pauli	53

II-3.3. Transformations unitaires	54
II-3.3.1. Diagonalisation	55
II-3.3.2. Changement de représentation	56
II-3.4. Les principes de la mécanique quantique	58

CHAPITRE III

Schola Quantorum : 2^e année

La dynamique quantique, la statistique quantique

III-1. Les équations du mouvement	61
III-1.1. L'équation de Schrödinger	61
III-1.2. Relation d'incertitude de Heisenberg	64
III-1.3. L'opérateur d'évolution	65
III-1.4. Les divers modes de description	67
III-1.4.1. Le mode de description de Schrödinger	67
III-1.4.2. Le mode de description de Heisenberg	68
III-2. La statistique quantique	71
III-2.1. La polarisation du photon	71
III-2.2. L'opérateur densité	75
III-2.2.1. Cas d'un état pur	75
III-2.2.2. Cas d'un mélange statistique	77
III-2.2.3. Trois remarques	79
III-2.3. Évolution de l'opérateur densité	83
III-2.4. Caractérisation de l'opérateur densité	84

CHAPITRE IV

Le qubit, unité élémentaire d'information quantique

IV-1. Le spin $\frac{1}{2}$	88
IV-1.1. Opérateur de rotation	88
IV-1.2. Rotation et moment cinétique	91
IV-1.3. Rotation des états de spin $\frac{1}{2}$	93
IV-2. Opérateur densité d'un qubit	97
IV-3. Portes logiques classiques, portes logiques quantiques	99
IV-3.1. Portes logiques classiques	99
IV-3.2. Portes logiques quantiques	106
IV-4. Préparation de qubits	110
IV-4.1. À partir de l'expérience de Stern et Gerlach	110
IV-4.2. Avec un champ magnétique constant	112
IV-4.3. Avec un champ magnétique tournant	113

CHAPITRE V

Deux qubits et plus si...

V-1. L'intrication	119
V-1.1. Notion d'intrication	119
V-1.2. Exemples d'intrication	120
V-1.2.1. Premier exemple : les états de Bell	120

V-1.2.2. Deuxième exemple : formation d'un état intriqué	122
V-1.2.3. Troisième exemple : critère de non-intrication	123
V-1.2.4. Quatrième exemple : d'un état intriqué à un état non intriqué	123
V-2. Mise en cause de la théorie quantique	124
V-2.1. L'argument EPR et le principe de complétude	124
V-2.2. Les inégalités de Bell	127
V-2.3. L'expérience d'Alain Aspect	130
V-2.4. Le chat de Schrödinger et la décohérence	132
V-3. Retour sur le formalisme de l'opérateur densité	134
V-3.1. L'opérateur densité réduit et l'opération trace partielle	134
V-3.2. Le théorème de Gleason	136
V-4. La décomposition et la purification de Schmidt	137
V-5. Portes quantiques à deux bits : la porte cNOT et les circuits associés	139
V-5.1. Permutation des états de deux qubits	140
V-5.2. Le théorème de non-clonage	140
V-5.3. Construction des états de Bell	141
V-5.4. Codage dense	142
V-5.5. La téléportation	143
V-6. Portes quantiques à trois qubits : la porte de Toffoli	144

CHAPITRE VI

Algorithmes de Deutsch-Jozsa et de Grover

VI-1. Les notions d'algorithme et de complexité	147
VI-1.1. Les notions de calculabilité et de décidabilité	147
VI-1.2. Machine de Turing classique	149
VI-1.3. Machine de Turing quantique	153
VI-1.4. Complexité des algorithmes	155
VI-2. L'algorithme de Deutsch-Jozsa	156
VI-2.1. Le problème de Deutsch	156
VI-2.2. Le problème de Deutsch-Jozsa	159
VI-2.3. Le problème de Bernstein-Vazirani	163
VI-2.4. Le problème de Simon	164
VI-3. L'algorithme de recherche de Grover	166
VI-3.1. L'oracle	167
VI-3.2. L'itération de Grover	168
VI-3.3. Exposé de la procédure suivi de deux applications	170
VI-3.3.1. La procédure	170
VI-3.3.2. « Un parmi quatre »	171
VI-3.3.3. « Un parmi huit »	172
VI-3.4. Le circuit quantique	173
VI-3.5. Recherche de plusieurs index	175
VI-3.6. Parenthèse sur le chiffre DES	176

CHAPITRE VII

Algorithme de Shor

VII-1. La transformée de Fourier quantique	177
VII-2. Période d'une fonction	184
VII-2.1. Calcul de la période	184
VII-2.2. La notion de fractions continues	189
VII-3. L'algorithme de Shor	191
VII-3.1. Un peu d'arithmétique modulaire	191
VII-3.2. Le problème de la factorisation	194
VII-3.3. La procédure	197
VII-3.4. Deux exemples	201
VII-4. Quantique et cryptographie	205
VII-4.1. Le système de cryptage RSA	206
VII-4.2. La distribution quantique de clés	209
VII-4.2.1. Le protocole BB84	210
VII-4.2.2. Le protocole EPR	213

CHAPITRE VIII

Bruits quantiques

Codes correcteurs d'erreurs quantiques

VIII-1. Opération quantique et opérateurs de Kraus	216
VIII-2. Bruits quantiques	219
VIII-2.1. La dépolarisation	219
VIII-2.2. Inversion de bit (bit flip), inversion de phase (phase flip)	221
VIII-2.3. Réduction d'amplitude	233
VIII-2.4. Saut de phase	225
VIII-3. Codes correcteurs d'erreurs quantiques	228
VIII-3.1. Code correcteur à trois qubits, cas de l'inversion de bit	229
VIII-3.1.1. La détection	230
VIII-3.1.2. La récupération	231
VIII-3.2. Code correcteur à trois qubits, cas de l'inversion de phase	233
VIII-3.3. Code correcteur de Shor à neuf qubits	233
VIII-3.4. Code correcteur à cinq qubits	237

CHAPITRE IX

Ordinateurs quantiques : avec quoi et comment ?

IX-1. Retour sur des considérations générales	241
IX-2. Quelques principes à suivre	244
IX-3. La résonance magnétique nucléaire ou RMN	248
IX-3.1. Le dispositif expérimental	251
IX-3.2. L'opérateur d'évolution	252
IX-3.2.1. Cas d'un spin dans un champ magnétique classique	252
IX-3.2.2. Couplage spin-spin	254
IX-3.2.3. À l'équilibre thermique	255

IX-3.2.4. Les signaux	256
IX-3.3. Construction de portes quantiques	258
IX-3.3.1. Portes à un qubit	258
IX-3.3.2. Porte cNOT	259
IX-3.3.3. La technique de refocalisation	260
IX-3.4. L'algorithme de Shor	261
IX-4. Les ions piégés	263
IX-4.1. Le dispositif expérimental	264
IX-4.2. L'opérateur d'évolution	270
IX-4.3. Construction de portes logiques	274
IX-4.4. Côté expérimental	277
IX-5. Ordinateurs photoniques	278
IX-5.1. Approche classique	279
IX-5.2. Approche quantique	283

CHAPITRE X

L'Univers, ordinateur quantique ultime

X-1. La physique quantique et le réalisme	289
X-2. La simulation quantique	291
X-3. La nature calcule	292
X-4. L'Univers ordinateur quantique	293
X-4.1. Son histoire	293
X-4.2. Sa capacité de calcul	295
X-5. Et maintenant ?	297
X-5.1. Mesure sans interaction et calcul contrefait	297
X-5.2. Calcul quantique topologique	298
X-5.3. Qu'en est-il ?	302

BIBLIOGRAPHIE	305
---------------	-----

INDEX	317
-------	-----