

G rard Fleury
Philippe Lacomme

Les algorithmes de base de

l'informaticque quantique

Grover, Shor et m taheuristiques
quantiques

Tome 2

●  ditions
EYROLLES

Éditions Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Depuis 1925, les éditions Eyrolles s'engagent en proposant des livres pour comprendre le monde, transmettre les savoirs et cultiver ses passions ! Pour continuer à accompagner toutes les générations à venir, nous travaillons de manière responsable, dans le respect de l'environnement. Nos imprimeurs sont ainsi choisis avec la plus grande attention, afin que nos ouvrages soient imprimés sur du papier issu de forêts gérées durablement. Nous veillons également à limiter le transport en privilégiant des imprimeurs locaux. Ainsi, 89 % de nos impressions se font en Europe, dont plus de la moitié en France.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans l'autorisation de l'Éditeur ou du Centre Français d'exploitation du droit de copie, 20 rue des Grands Augustins, 75006 Paris.

© Éditions Eyrolles, 2023

ISBN : 978-2-416-01172-6

AVANT-PROPOS

Nous avons introduit dans un livre précédent les éléments de base de l'informatique quantique en présentant les portes et en détaillant leur utilisation avec des calculs réalisés le plus souvent sous forme matricielle. Dans celui-ci nous présentons de façon détaillée des algorithmes "historiques" et des métaheuristiques quantiques (plus récentes) en mettant l'accent sur les fondements physiques et mathématiques de ces algorithmes.

Ce que l'informatique quantique promet de faire, c'est de résoudre plus vite des problèmes en les modélisant différemment.

Feynman a posé les bases du calcul quantique il y a plusieurs décennies, et des travaux algorithmiques ont été publiés dans les années 1990 par plusieurs chercheurs. Ils sont essentiellement connus grâce à deux algorithmes :

- celui de Grover ;
- celui de Shor.

L'algorithme de Grover est certainement le plus connu des chercheurs ou ingénieurs en informatique car il permet de rechercher un élément dans un tableau non trié, sans parcourir la totalité des cases du tableau et promet une accélération quadratique du processus. Comme la recherche dans un tableau est un des piliers de l'algorithmique, on comprend dès lors que sa capacité à fournir rapidement un résultat cohérent sans parcourir l'ensemble des données, ait pu attirer l'attention des informaticiens.

Alors que la renommée de l'algorithme de Grover est restée limitée aux informaticiens, celle de l'algorithme de Shor a largement dépassé la presse spécialisée et on retrouve dans la presse grand public de nombreux articles détaillant l'intérêt de cet algorithme. Ce dernier promet de factoriser un grand nombre en temps polynomial. Pour le non spécialiste cela peut sembler d'un

intérêt limité. Toutefois, la plupart des systèmes de cryptographie actuels sont fondés sur la factorisation d'un grand nombre. Plus précisément, ce qui rend difficile de casser un algorithme de cryptographie c'est le fait qu'il n'existe pas (a priori) d'algorithme efficace pour factoriser un nombre. Trouver un tel algorithme polynomial remet donc en cause la sécurité de la cryptographie. On comprend alors l'émoi et l'intérêt provoqués dans les années 1990 par la publication de l'algorithme de Shor.

Ces deux algorithmes font partie de ceux à connaître lorsque l'on souhaite approfondir ses connaissances en quantique. Mais leur compréhension nécessite de s'appropriier les notions indispensables en calculs tensoriels et en manipulation de portes quantiques.

La moitié de ce livre environ leur est consacrée avec essentiellement un objectif pédagogique pour permettre au lecteur de s'appropriier les notions essentielles. Un total de 4 algorithmes issus des années 1990 sont décrits et testés. Nous montrons que les expérimentations numériques donnent des résultats cohérents avec ce que prédit la théorie.

Depuis le début des années 2000, une nouvelle classe de méthodes quantiques a vu le jour. Il s'agit de métaheuristiques quantiques. Elles permettent de parcourir efficacement un espace des solutions et, de ce point de vue elles complètent ce qui se fait couramment en optimisation avec des méthodes telles que le recuit simulé, les algorithmes génétiques ou le GRASP.

Leur justification repose sur des concepts issus de la physique comme la notion d'Hamiltonien. Le livre contient les rappels indispensables à leur bonne compréhension et montre ensuite comment réaliser des implémentations efficaces pour les méthodes adiabatiques et celles de type QAOA.

Il est bien connu que la clé pour réussir efficacement l'exploration d'un espace de recherche de grande taille repose en partie sur la capacité à en explorer une partie susceptible de contenir une solution optimale. Des avancées récentes (2018) montrent comment, pour certains problèmes de Recherche Opérationnelle, on peut limiter efficacement l'exploration.

Le **chapitre 1** donne les fondements mathématiques sur lesquels reposent les calculs réalisés sur les ordinateurs quantiques et il introduit (en la justifiant) la sphère de Bloch comme un outil de visualisation.

Le **chapitre 2** constitue une introduction à l'algorithme de Deutsch-Jozsa qui permet d'identifier si une fonction est équilibrée ou non. Il est essentiellement théorique et assez éloigné d'une application réelle, mais il définit les éléments de base pour l'algorithme de Simon présenté dans le chapitre 3.

Le **chapitre 3** présente l'algorithme de Simon qui, lui, s'intéresse à la recherche d'un vecteur a tel que $f(x + a) = f(x)$ où f est une fonction qui associe à une chaîne de n bits une chaîne de $n - 1$ bits. En résumé, il s'agit de trouver deux entrées distinctes de n qubits qui correspondent à la même sortie.

Le **chapitre 4** donne une justification théorique complète de l'algorithme de Shor et montre comment la notion de phase (présentée au chapitre 1) permet de réaliser "facilement" les opérations élémentaires.

Le **chapitre 5** constitue une introduction à l'algorithme de Grover qui est probablement l'un des plus connus et qui permet de trouver un élément dans un tableau sans en parcourir toutes les cases.

Le **chapitre 6** contient des compléments utiles de mathématiques et de physiques pour mieux comprendre les justifications théoriques telles que la notion d'Hamiltonien et d'optimisation adiabatique.

Le **chapitre 7** propose des compléments pour approfondir les notions abordées dans les chapitres précédents.

Le **chapitre 8** contient les annexes.

Remarques importantes

1) Dans ce livre, le séparateur décimal utilisé est le point (".") et le livre reprend, généralement, les conventions anglo-saxonnes.

- 2) Les chapitres doivent être lus, de préférence, dans l'ordre proposé. Toutefois, pour permettre une lecture dans un ordre différent, certaines notions nécessaires à la compréhension d'un chapitre sont parfois résumées au début de celui-ci.
- 3) Toujours pour permettre une lecture dans un ordre quelconque, les chapitres comportent, à différents endroits, un résumé des notions précédemment introduites.

Les programmes accompagnant ce livre sont disponibles sur Internet à l'adresse suivante :

http://www.isima.fr/~lacomme/Quantique_Livre_2/index.php

Ces programmes sont libres, vous pouvez les redistribuer et/ou les modifier selon les termes de la Licence Publique Générale GNU publiée par la Free Software Foundation (version 2 ou bien toute autre version ultérieure choisie par vous).

Vous pouvez contacter les auteurs en utilisant les adresses suivantes :

Gérard Fleury : gerard.fleury@isima.fr

Philippe Lacomme : placomme@isima.fr

SOMMAIRE

Chapitre 1.....	Les notions de base
1.1	Introduction 17
1.2	Liens entre S^2 and $SU(2)$ 26
1.3	Les relations entre $SO(3)$ et $SU(2)$ 43
1.4	Conclusion 54
1.5	Références 55
Chapitre 2.....	Algorithme de Deutsch-Jozsa
2.1	Calculs tensoriels 57
2.2	Définition du problème de Deutsch-Jozsa 70
2.3	Oracle de Deutsch-Jozsa 71
2.4	Généralisation à une fonction quelconque 85
2.5	Évaluation numérique du circuit pour une fonction balancée quelconque 94
2.6	Évaluation numérique du circuit pour une fonction constante 97
2.7	Évaluation numérique du circuit pour une fonction non balancée et non constante..... 98
2.8	Conclusion 100
2.9	Références 100
Chapitre 3.....	Algorithme de Simon
3.1	Définition du problème de Simon..... 101
3.2	Algorithme de Simon..... 103
3.3	Exemple 120
3.4	Simon : le circuit conceptuel ($n = 2$)..... 124
3.5	Simon : le circuit "effectif" dans le cas général $k \geq 2$ 130
3.6	Circuit et calculs condensés pour l'algorithme de Simon : $n = 2$ 134
3.7	Circuit et calculs condensés pour l'algorithme de Simon : $n = 3$ 140
3.8	Conclusion 157
3.9	Références 157
Chapitre 4.....	Algorithme de Shor
4.1	Principes de base..... 159
4.2	Algorithme de Shor..... 168

4.3	Exemple complet avec $N = 15$ ($p = 4$) et $a = 2$	180
4.4	Exemple complet avec $N = 15$ ($p = 8$) et $a = 2$	186
4.5	Exemple avec $N = 33$ ($p = 11$) et $a = 7$	192
4.6	Exemple avec $N = 33$ ($p = 11$) et $a = 2$	193
4.7	Conclusion.....	199
4.8	Algorithme de Shor avec utilisation de la phase.....	200
4.9	Évaluations numériques pour $N = 33$	214
4.10	Conclusion.....	220
4.11	Références.....	221

Chapitre 5.....Algorithme de Grover

5.1	Notion de phase et analyse des portes X et H	223
5.2	Analyse et interprétation du circuit.....	230
5.3	Exemple d'application de l'algorithme de Grover.....	252
5.4	Conclusion.....	260
5.5	Références.....	260

Chapitre 6.....Métaheuristiques quantiques

6.1	Notion d'opérateur et d'Hamiltonien.....	261
6.2	Un problème SAT modélisé sous la forme d'un Hamiltonien.....	276
6.3	Modélisation d'un problème de MaxCut.....	281
6.4	Modélisation d'un problème de partitionnement de nombres.....	284
6.5	Modélisation d'un problème de coloration de graphe.....	287
6.6	Modélisation d'un problème de TSP.....	289
6.7	Implémentation des circuits quantiques des Z_i	292
6.8	Optimisation adiabatique.....	297
6.9	Résolution d'un problème 3-SAT à trois clauses et trois variables.....	306
6.10	Résolution d'un problème de MaxCut.....	311
6.11	QAOA.....	313
6.12	Résolution d'un problème de MaxCut avec QAOA.....	316
6.13	Résolution d'un problème de coloration de graphe avec QAOA.....	333
6.14	Conclusion.....	337
6.15	Références.....	337

Chapitre 7	Compléments
7.1 Généralités sur les Hamiltoniens	339
7.2 Hamiltonien d'une masse avec ressort	365
7.3 Définition d'un Hamiltonien : Synthèse à retenir.....	377
7.4 Conclusion	378
7.5 Références	378
Chapitre 8*	Annexes
8.1 Interprétation tensorielle de la transformée de Fourier.....	381
8.2 Représentation du Spin	389
8.3 Exponentielle et changement de base	397
8.4 Conclusion.....	407
8.5 Références	407
Index	409

* : le chapitre 8 est un complément téléchargeable sur le site du livre :

http://www.isima.fr/~lacomme/Quantique_Livre_2/index.php

