Gérard Fleury
Philippe Lacomme

Les algorithmes de base de l'informatique quantique

Grover, Shor et métaheuristiques quantiques

Tome 2

Éditions EYROLLES

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

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'approprier 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'approprier 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 balancée 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

Vous pouvez contacter les auteurs en utilisant les adresses suivantes :

Gérard Fleury : gerard.fleury@isima.fr

Philippe Lacomme : placomme@isima.fr

SOMMAIRE

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

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