Évaluation du potentiel des machines quantiques pour l'optimisation combinatoire

Julien Rodriguez

CEA-LIST, Palaiseau, France
julien.rodriguez@cea.fr

LIRMM, Montpellier, France (Stage)
Université de Montpellier (Master 2)

Mots-clés : *recherche opérationnelle quantique, optimisation.*

1 Introduction

L'arrivée des machines quantiques risque de révolutionner de nombreux domaines, en particulier celui des algorithmes combinatoires. Cette étude propose d'évaluer la performance des algorithmes existants (et publiés) et d'éclairer les opportunités des algorithmes quantiques. De plus, il est proposé une introduction à l'informatique quantique à partir de zéro et fourni les connaissances nécessaires à tout informaticien désireux de réaliser des circuits quantiques. Dans un premier temps, il est présenté l'algorithme de recherche dans une base non structurée de Lov Grover (1996) [2] ainsi que deux autres algorithmes inspirés de l'algorithme de Grover traitant le problème de satisfiabilité d'une formule logique et la recherche d'éléments dans un tableau. De plus, chaque circuit présenté est accompagné d'une illustration concrète du circuit (qubits, portes, etc.) et d'une implémentation en accès libre, disponible sur le git du LIRMM [1]. Dans beaucoup de documents, le circuit présenté par Giacomo Nannicini dans [5] traitant le problème *exact 1-3 SAT* est présenté comme une voie vers un circuit pour le problème 3-SAT et plus généralement SAT. Notre première contribution a été de réaliser un circuit expliqué étape par étape en s'abstrayant de la physique [2], pour le problème SAT.

2 Recherche opérationnelle quantique

Avec un circuit pour le problème SAT, nous pouvions commencer à traiter des problèmes d'optimisation combinatoire. Mais avec le faible nombre de qubits disponibles ($\simeq 50$), il est difficile de représenter certains problèmes d'optimisation en une formule SAT. L'approche a donc été de construire des algorithmes opérants directement sur des registres encodant des valeurs entières en représentation binaire avec les opérateurs : $+$,$-$,$<$,$>$,$\neq$,*table* [1, 6, 7, 8] .

2.1 Couverture de sommets de poids minimal

Pour un graphe $G = (V, E, w)$, résoudre le problème de la couverture minimale revient à trouver un ensemble de sommets $S \subset V$ permettant de couvrir toutes les arêtes de G tout en minimisant la somme des poids des sommets dans S. Ce problème est NPC [4]. À partir du circuit pour SAT et des circuits $+$, $<$ et *table*, le problème peut s'écrire comme :

$$\min \sum_{1}^{n} x_i w_i$$

1. https ://gite.lirmm.fr/bourreau/quantumgroversearch
2. Dans la même démarche que Giacomo Nannicini : *An Introduction to Quantum Computing, Without the Physics* [5]

$$st. \sum_{(u,v)\in E} (x_u \vee x_v) > 0$$

Où w_i est le poids du sommet i, x_i une variable binaire indiquant si le sommet i appartient à la couverture et les contraintes $(x_u \vee x_v) > 0$ imposent que la couverture du graphe soit totale. Le circuit associé à ce problème a été généré et exécuté avec succès afin de valider la réalisabilité de l'encodage d'un problème NPC. Il est disponible en ligne comme première brique d'une recherche opérationnelle quantique.

2.2 Autres problèmes

Nos autres contributions ont été de fournir des circuits pour la recherche dichotomique dans un tableau, la coupe maximum et le voyageur de commerce avec une complexité de l'ordre de $O(n\sqrt{2^n})$. Comme l'algorithme de Grover permet de chercher dans une base non structurée en $O(\sqrt{2^n})$, la recherche dichotomique quantique va itérativement chercher les valeurs inférieures ou supérieures à un entier $k = max_{val}/2$ et appellera Grover au plus n fois. Les autres algorithmes étant basés sur la recherche dichotomique ils sont du même ordre de complexité.

La complexité connue de Held et Karp pour le problème du voyageur de commerce en recherche exacte est de l'ordre de $O(n^2.2^n)$ [3]. Comme le voyageur de commerce quantique admet une complexité de $O(n2^{\frac{n}{2}})$, la version quantique apporte une accélération quadratique.

3 Conclusions et perspectives

À l'heure actuelle les machines ne sont pas encore assez fiables pour obtenir des résultats. Cependant, il est possible d'utiliser le simulateur que nous avons poussé jusqu'au *timeout* constructeur sur une instance du voyageur de commerce. En 2020, le nombre de qubits disponibles ne permet pas de modéliser des instances comparables en taille à celles exécutées sur machine séquentielle. Selon la courbe prévisionnelle d'IBM, les machines devraient atteindre une fiabilité acceptable et un nombre de qubits suffisant d'ici 2030. Cette évolution permettrait d'évaluer la présence ou non d'une transition de phase pour le problème SAT quantique et aussi de traiter des problèmes plus contraint demandant plus de qubits pour la modélisation (VRP, Eternity II, ...).

Références

[1] Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin, and David Petrie Moulton. A new quantum ripple-carry addition circuit, 2004.

[2] Lov K. Grover. Quantum Computers Can Search Rapidly by Using Almost Any Transformation. 80(19) :4329–4332, May 1998.

[3] Michael Held and Richard M. Karp. A dynamic programming approach to sequencing problems. *Journal of the Society for Industrial and Applied Mathematics*, 10(1) :196–210, 1962.

[4] Richard M. Karp. *Reducibility among Combinatorial Problems*, pages 85–103. Springer US, Boston, MA, 1972.

[5] Giacomo Nannicini. An introduction to quantum computing, without the physics, 2017.

[6] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*, volume 1. Cambridge University Press, 2010.

[7] David Oliveira and Rubens Ramos. Quantum bit string comparator : Circuits and applications. *Quantum Computers and Computing*, 7, 01 2007.

[8] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Physical Review A*, 54(1) :147–153, Jul 1996.