

G rard Fleury
Philippe Lacomme

Algorithmes efficaces de l'informatique quantique



Références sciences

Algorithmes efficaces de l'informatique quantique

Gérard Fleury
Philippe Lacomme



Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

*Retrouvez tous les livres de la collection
et des extraits sur www.editions-ellipses.fr*



ISBN 9782340-116559

Dépôt légal : octobre 2026

©Ellipses Édition Marketing S.A.

8/10 rue la Quintinie 75015 Paris



Le Code de la propriété intellectuelle et artistique n'autorisant, aux termes des alinéas 2 et 3 de l'article L. 122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'article L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

PRÉFACE

Il m'a été demandé d'écrire la préface de cet ouvrage consacré aux *algorithmes efficaces de l'informatique quantique*. J'y ai consenti avec enthousiasme, mais aussi avec humilité car je ne suis pas un spécialiste du quantique. Mon parcours s'inscrit avant tout dans le champ des mathématiques appliquées, de la recherche opérationnelle, et de l'optimisation ; des domaines dans lesquels j'évolue depuis de nombreuses années. C'est donc du point de vue d'un "néophyte éclairé", curieux mais extérieur au quantique, que j'aborde ce livre.

Dès les premiers instants de lecture, on voit combien l'univers présenté ici résonne avec les préoccupations des chercheurs en mathématique et plus particulièrement en optimisation. C'est d'ailleurs aussi celui des auteurs. Derrière le formalisme propre au quantique, on retrouve des structures familières : espaces vectoriels, opérateurs linéaires, exponentielles de matrices, modélisations énergétiques, et bien sûr, ce lien intime entre la structure mathématique d'un problème et l'efficacité des méthodes employées pour le résoudre.

L'une des forces de cet ouvrage est précisément de s'adresser à un lectorat qui n'est pas nécessairement formé aux concepts fondamentaux de la mécanique quantique. Dès le premier chapitre, les auteurs prennent soin de rappeler les bases mathématiques sur lesquelles repose l'algorithmique quantique : définition du qubit, états superposés, portes de Pauli, produits tensoriels, opérateurs unitaires et Hamiltoniens. Cette démarche pédagogique permet à un lecteur issu de l'optimisation ou de l'informatique de trouver ses repères et de comprendre progressivement la logique interne des calculs quantiques.

Ce préambule est essentiel, car la suite du livre montre à quel point l'algorithmique quantique repose sur une articulation subtile entre structure mathématique, capacité de modélisation et puissance de calcul potentielle. Contrairement aux présentations souvent focalisées sur les "algorithmes vedettes" tels que Shor ou Grover, les auteurs ont choisi de proposer au lecteur un panorama large des approches permettant d'utiliser efficacement les machines quantiques actuelles, des machines encore limitées en nombre de qubits, mais dont les principes de programmation préfigurent des ruptures profondes.

Le fil conducteur de l'ouvrage est clair : comprendre comment traduire un problème classique en un formalisme quantique adapté, et comment exploiter les mécanismes fondamentaux du calcul quantique pour en améliorer la résolution. Cette idée se décline de manière particulièrement convaincante dans deux directions majeures :

L'utilisation de l'algorithme d'estimation de phase (QPE) et ses applications à des problèmes comme le TSP ou les systèmes linéaires ;

L'étude des méthodes itératives de type adiabatique ou QAOA, qui reposent sur la construction d'Hamiltoniens soigneusement conçus et l'application à des problèmes de coloration de graphes ou de minimisation d'une fonction.

Les chapitres consacrés à QPE illustrent admirablement comment un algorithme d'apparence très théorique devient un outil d'optimisation lorsqu'il est associé à des opérateurs explicitement construits. Les auteurs ne se contentent pas de décrire le cadre général : ils détaillent la manière de coder un opérateur, de représenter les matrices diagonales, puis de mettre en œuvre l'algorithme sur des exemples concrets tels qu'un TSP à quatre sommets. Pour un lecteur habitué à la recherche opérationnelle, ce choix est extrêmement pertinent. Il montre que l'enjeu principal n'est pas l'algorithme en lui-même, mais la qualité et la pertinence de la modélisation quantique du problème.

Cette idée revient avec encore plus de force dans les chapitres consacrés à l'optimisation adiabatique et aux Drivers Hamiltoniens. Le livre montre comment la définition du bon Hamiltonien, c'est-à-dire celui dont les plus petites valeurs propres correspondent aux solutions recherchées, conditionne entièrement la réussite de l'algorithme. Les auteurs proposent des techniques de construction et de réécriture d'Hamiltoniens, notamment pour le cas de la coloration de graphe, du TSP ou même d'un problème SAT. Ces passages sont particulièrement précieux pour les lecteurs issus de la modélisation : ils démontrent que l'élaboration d'un Hamiltonien efficace est une étape conceptuelle proche de la création d'un modèle mathématique robuste dans les méthodes d'optimisation classiques, mais enrichie ici d'une dimension physique nouvelle.

Le chapitre consacré aux techniques de quadratisation ou à l'utilisation d'une solution heuristique comme point de départ ("warm start") constitue à mes yeux l'un des apports les plus stimulants de l'ouvrage. On y retrouve des intuitions familières : réduire la taille du problème, tirer parti d'une structure a priori, limiter l'exploration inutile. Mais ces intuitions doivent être reformulées dans un langage quantique, ce qui ouvre des perspectives passionnantes pour les chercheurs en optimisation : comment repenser nos heuristiques, nos relaxations, nos méthodes de décomposition, pour les adapter à des machines quantiques encore imparfaites, mais prometteuses ?

L'un des mérites de ce livre est également de maintenir une grande honnêteté scientifique. À plusieurs reprises, les auteurs rappellent que les performances

actuelles des ordinateurs quantiques ne rivalisent pas encore avec celles des meilleures méthodes classiques, tant en taille d'instances résolues qu'en qualité des solutions obtenues. Ce constat, loin d'être décourageant, permet au contraire de situer précisément l'état de l'art, d'éviter les discours sensationnalistes et de concentrer l'intérêt du lecteur sur ce qui constitue véritablement le cœur du progrès : l'amélioration des modélisations, l'efficacité des méthodes, la compréhension profonde des structures mathématiques sous-jacentes.

Les lecteurs qui connaissent déjà les auteurs retrouveront avec plaisir leur goût pour l'illustration concrète par le code. Les nombreux extraits d'implémentations proposés au fil des chapitres viennent appuyer les explications théoriques et les démarches de résolution. Ils montrent surtout qu'il est aujourd'hui possible de programmer des algorithmes quantiques, d'en observer le comportement et d'en extraire des solutions exploitables, même si cela se fait pour des instances de taille modeste.

En définitive, ce livre a ceci d'unique qu'il fait dialoguer deux mondes : celui des physiciens et informaticiens quantiques, et celui des chercheurs opérationnels et mathématiciens appliqués. Pour le lecteur néophyte mais investi, le voyage est exigeant, parfois déroutant, mais toujours guidé et éclairé. Pour le lecteur expert, il offre une synthèse remarquable et des perspectives méthodologiques très riches.

Quant à moi, j'y ai trouvé une invitation à repenser les frontières de notre discipline : ce que nous appelions jadis calcul ou optimisation acquiert ici une profondeur nouvelle, liée aux principes fondamentaux de la nature. Les méthodes présentées dans cet ouvrage préfigurent peut-être les outils qui, demain, permettront de résoudre des problèmes que nous pensons aujourd'hui inabordables.

Je souhaite donc au lecteur la même curiosité enthousiaste que celle qui m'a accompagné tout au long de ces pages. Je remercie chaleureusement les auteurs pour cet ouvrage ambitieux, rigoureux et généreux, qui contribue à ouvrir un champ encore émergent mais déjà essentiel : celui des modélisations efficaces pour l'informatique quantique.

Marc Sevaux

Le 5 décembre 2025

AVANT-PROPOS

Le lecteur peut trouver aisément la description des algorithmes classiques de l'informatique quantique tels que Shor et Grover dans de nombreux ouvrages dont la plupart sont en anglais et parfois en français.

Ce que l'informatique quantique permet de faire, c'est de résoudre des problèmes complexes à condition de modéliser correctement le problème de départ pour appliquer correctement des méthodes de résolution. Les méthodes que l'on retrouve classiquement sont généralement issues de la physique et définissent des approches génériques de résolution.

Avec ces méthodes, il est possible de résoudre efficacement des problèmes complexes mais, lorsque l'on compare la taille des instances résolues avec des approches classiques à celles résolues avec des approches quantiques, la comparaison n'est pas encore en faveur des machines quantiques qui possèdent encore trop peu de qubits. Un constat presque similaire s'applique aussi à l'analyse des résultats. Lorsque l'on compare la qualité des solutions trouvées avec des approches quantiques aux solutions obtenues en utilisant les meilleures méthodes actuelles non quantiques, la comparaison n'est pas toujours en faveur des approches quantiques... même sur de petites ou moyennes instances.

Pour obtenir des implémentations quantiques efficaces, il faut maîtriser des outils qui permettent d'adapter les modélisations et les processus de résolution aux problèmes à résoudre. Ce livre se propose donc de parcourir un ensemble plus vaste de méthodes et de s'intéresser à la conception de méthodes adaptées aux problèmes, ou tout au moins d'expliquer comment "adapter" les méthodes et les modélisations.

Améliorer les modélisations repose essentiellement sur deux voies possibles :

- des techniques de réécriture de l'Hamiltonien afin de faciliter sa réécriture : ces notions sont abordées au chapitre 8;
- des techniques qui permettent de contrôler l'exploration de l'espace (en se limitant aux qubits -strings modélisant des solutions) et de tirer profit de solutions connues a priori de bonne qualité. Ces notions sont abordées au chapitre 7.

Le livre se compose de 8 chapitres.

Le **chapitre 1** rappelle les bases mathématiques indispensables pour aborder les chapitres suivants du livre. Il introduit la notion de portes quantiques, il définit les vecteurs propres et valeurs propres. Il rappelle aussi les éléments de calcul tensoriel

et définit la notion d'Hamiltonien. Il contient enfin une introduction aux principes de résolution basées sur une approche adiabatique.

Le **chapitre 2** donne les fondements mathématiques de l'algorithme QPE pour Quantum Phase Estimation. Il s'agit d'une présentation qui concerne essentiellement les fondements théoriques. Ce chapitre contient la description du circuit quantique avec les calculs associés.

Le **chapitre 3** constitue une application de QPE à un problème de TSP. Il détaille à la fois le problème de codage et la traduction de U . L'application numérique concerne un TSP à 4 sommets. L'application numérique montre que connaissant un vecteur propre, le circuit permet de "trouver" le coût associé.

Le **chapitre 4** aborde les calculs sous l'angle des calculs tensoriels et rappelle les éléments fondamentaux à maîtriser sur le sujet. Le point important du chapitre concerne le calcul des exponentielles complexes pour lesquelles le chapitre donne un algorithme permettant d'obtenir, pour une exponentielle complexe, le circuit quantique associé.

Le **chapitre 5** s'intéresse à la résolution de système d'équations linéaires avec la méthode HHL. La résolution de systèmes linéaires a suscité un grand intérêt de la communauté scientifique et a donné lieu à la création de solveurs dédiés. Ceci explique l'importance de la méthode HHL que le chapitre décrit d'abord sous un angle théorique et ensuite pratique via plusieurs mises en œuvre. La difficulté principale de la méthode réside dans le calcul d'une quantité de la forme x/y et les mises en œuvre sont limitées à des formes simples de x/y .

Le **chapitre 6** aborde un point difficile lié à la mise en œuvre de HHL à savoir le calcul d'une fraction x/y dans le cas général.

Le **chapitre 7** concerne la définition de Driver Hamiltonien spécifique à chaque problème d'optimisation car c'est un élément important de la mise en œuvre efficace des méthodes itératives de type QAOA ou Adiabatique. Ce chapitre est consacré au premier Driver Hamiltonien ayant donné lieu à une mise en œuvre sur des cas pratiques et qui a été proposé par Hadfield en 2018. Son domaine d'application principal concerne les problèmes de coloration de graphe.

Le **chapitre 8** s'intéresse aux techniques de réécriture d'Hamiltonien qui peuvent permettre d'obtenir des implémentations différentes et influencent la convergence des méthodes itératives de résolution abordées au chapitre 6. Ces techniques sont analysées sur un problème SAT à travers un exemple numérique complet.

Remarques

- 1) Dans ce livre, le séparateur décimal utilisé est le point (".") et les conventions anglo-saxonnes sont privilégiées. Ainsi le livre utilise les guillemets anglosaxons en lieu et place des guillemets français car c'est l'usage le plus répandu dans les publications scientifiques car elles facilitent la lecture de texte comprenant des formules mathématiques.
- 2) Pour faciliter une lecture dans un ordre quelconque des chapitres, certaines notions nécessaires à la compréhension d'un chapitre sont parfois résumées au début de celui-ci.
- 3) Les chapitres sont de difficultés croissantes.

Vous pouvez contacter les auteurs en utilisant les adresses suivantes :

Gérard Fleury : gerard.fleury@isima.fr et gyf@sfr.fr

Philippe Lacomme : placomme@isima.fr

À QUI S'ADRESSE CE LIVRE ?

- Aux **élèves d'écoles d'ingénieurs en informatique** qui ont des cours sur des problèmes d'optimisation et qui souhaitent compléter les approches classiques par des approches quantiques.
- Aux **ingénieurs dans les centres de R&D** qui souhaitent se former à ce qui est en train de devenir une nouvelle voie de recherche.
- Aux **enseignants** qui souhaitent ouvrir de nouveaux cours et TP.

Remerciements

Ce livre n'aurait pas vu le jour sans l'aide amicale de nos collègues avec qui nous avons régulièrement des discussions techniques autour du quantique. Avec l'arrivée du EURO Working Group la communauté qui s'est constituée, a créé une émulation importante et un enthousiasme qui nous a accompagnés tout au long de la rédaction.

Gérard Fleury, Philippe Lacomme

SOMMAIRE

Chapitre 1 Concepts généraux

1.1	Concepts mathématiques de base	15
1.2	Eléments propres des portes de Pauli	22
1.3	Calcul tensoriel.....	23
1.4	Exponentielle.....	25
1.5	Notion d'Hamiltonien	25
1.6	Meta-Heuristiques Quantiques	29
1.7	Conclusion.....	31
1.8	Références	31

Chapitre 2 Algorithme d'Estimation de la Phase

2.1	Présentation	33
2.2	Application	44
2.3	Vecteurs propres pour les opérateurs de la forme e^{iA}	60
2.4	Précision obtenue à la fin de la transformée de Fourier	71
2.5	Conclusion.....	74
2.6	Références	75

Chapitre 3 Application de QPE à la résolution du TSP

3.1	Représentation des opérateurs diagonaux	77
3.2	Résolution du TSP à 4 sommets avec QPE.....	81
3.3	Conclusion.....	92

Chapitre 4 Calculs tensoriels

4.1	Exponentiation d'opérateurs	93
4.2	Automatisation des calculs de $e^{-i.t.H}$	118
4.3	Codages pour les circuits quantiques	132
4.4	Tomographie quantique.....	143
4.5	Conclusion.....	153
4.6	Références	153

Chapitre 5 Application de QPE à la résolution de systèmes linéaires

5.1	Résolution d'un système d'équations linéaires avec QPE.....	155
5.2	Description de HHL	167
5.3	Mise en œuvre de HHL sur un exemple simple	200
5.4	Mise en œuvre de HHL sur un deuxième exemple	204
5.5	Application de HHL avec la méthode ExactReciprocal.....	206
5.6	Conclusion.....	208
5.7	Références	208

Chapitre 6 Méthode de calcul numérique

6.1	Calculs exacts	211
6.2	Calculs approchés.....	231
6.3	Conclusion.....	232
6.4	Références	232

Chapitre 7 Drivers Hamiltoniens pour l'optimisation adiabatique

7.1	Notion de qudit.....	233
7.2	Meta-Heuristiques Quantiques	255
7.3	Hamiltonien	260
7.4	Analyse du cas particulier $H_D = \sum_{i=0}^n \frac{1}{2} (X_i \cdot X_{i+1} + Y_i \cdot Y_{i+1})$	278

7.5	Problème de coloration de graphe	295
7.6	Application à la minimisation d'une fonction à deux variables.....	306
7.7	Application à la minimisation d'une fonction à 4 variables	312
7.8	Conclusion.....	320
7.9	Références	320

Chapitre 8 Techniques d'optimisation des fonctions

8.1	Résolution du TSP (Travelling Salesman Problem).....	323
8.2	Définition d'un Driver Hamiltonian H_B	328
8.3	Tirer profit d'une solution "heuristique"	342
8.4	Mise en œuvre pour un TSP à 5 sommets	345
8.5	QAOA avec "warm start" pour un TSP à 5 sommets.....	353
8.6	Techniques de quadratisation	356
8.7	Un problème SAT modélisé sous la forme d'un Hamiltonien	373
8.8	Conclusion.....	380
8.9	Références	380

Index 383

CHAPITRE 1

Concepts généraux

Objectifs : le livre est organisé de telle sorte que les concepts sont introduits au fur et à mesure dans les chapitres où ils sont indispensables. Ce chapitre est donc un résumé des notions de base qui sont manipulées par la suite.

1.1 Concepts mathématiques de base

1.1.1 Notion de qubit

Un qubit est l'unité élémentaire de calcul défini par :

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

avec $|\alpha|^2 + |\beta|^2 = 1$ et α, β sont deux valeurs complexes.

1.1.2 Etat quantique

Un état $|\psi\rangle$ est défini par la superposition des différents états qui entrent dans la définition de $|\psi\rangle$. Donc $|\psi\rangle$ peut être défini par un tenseur de rang N avec $\sum_{n_1 n_2 n_3 \dots n_N} |\psi^{n_1 n_2 n_3 \dots n_N}|^2 = 1$.

Si l'on néglige les corrélations quantiques, alors la fonction d'onde peut être définie comme le produit de N fonctions d'onde, chaque fonction étant définie sur un espace de dimension d .

$$|\psi\rangle = |\psi^1\rangle \otimes |\psi^2\rangle \otimes \dots \otimes |\psi^N\rangle$$

Ou encore

$$|\psi\rangle = \sum_{\alpha_1=1}^d \psi_{\alpha_1} |\alpha_1\rangle \otimes \sum_{\alpha_2=1}^d \psi_{\alpha_2} |\alpha_2\rangle \otimes \dots \otimes \sum_{\alpha_N=1}^d \psi_{\alpha_N} |\alpha_N\rangle$$

Un état $|\psi\rangle$ est défini par la superposition des différents états qui entrent dans la définition de $|\psi\rangle$.

$$|\psi\rangle = \sum_{n_1 n_2 n_3} \psi^{n_1 n_2 n_3} \cdot |n_1 n_2 n_3\rangle$$

Avec

$|\psi^{n_1 n_2 n_3}|^2$ qui donne la probabilité d'observer le système dans la configuration $n_1 n_2 n_3$

Un opérateur est simplement défini par une matrice avec un ensemble de coefficients $O_{n'_1 n'_2 n'_3}^{n_1 n_2 n_3}$ où $n_1 n_2 n_3$ sont des indices de ligne qui font référence au primal et $n'_1 n'_2 n'_3$ sont des indices de colonne qui font référence au dual.

Ainsi :

$$O = \sum_{n_1 n_2 n_3} O_{n'_1 n'_2 n'_3}^{n_1 n_2 n_3} |n_1 n_2 n_3\rangle \langle n'_1 n'_2 n'_3|$$

Il est possible d'introduire alors la définition de

$$\langle\psi|\phi\rangle = \sum_{n_1 n_2 n_3, n'_1 n'_2 n'_3} \psi_{n_1 n_2 n_3} \cdot \phi^{n'_1 n'_2 n'_3}$$

On peut alors définir la valeur moyenne de O :

$$\langle\psi|O|\phi\rangle = \sum_{n_1 n_2 n_3} \psi_{n_1 n_2 n_3} \cdot O_{n'_1 n'_2 n'_3}^{n_1 n_2 n_3} \cdot \phi^{n'_1 n'_2 n'_3}$$

1.1.3 Les portes quantiques

Les portes quantiques correspondent aux instructions qu'on trouve dans les langages de programmation classiques tels que le C ou le C++. Elles jouent un rôle très important car elles servent à définir des circuits quantiques sont eux le pendant des programmes dans l'informatique traditionnelle. Nous rappelons ci-dessous quelques éléments de base. Leur matrice dans la base $(|0\rangle, |1\rangle)$, est pour :

La porte $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

La porte $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

La porte $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

La porte $H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

La porte $\frac{\pi}{8} = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Les trois premières portes sont appelées portes de Pauli.

Sauf mention du contraire, dans ce qui suit, la matrice d'un opérateur est donnée dans la base ($|0\rangle, |1\rangle$)

A partir de ces portes on peut définir des portes contrôlées de la forme par exemple :

CX_{ij} : Control- X

CZ_{ij} : Control- Z

Ces portes signifient qu'on applique la porte sur le qubit j si le qubit i défini comme le qubit de contrôle vaut 1.

1.1.4 La porte quantique de Hadamard

Elle se définit par : $H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Il est possible de l'appliquer à $|0\rangle$, ce qui donne :

$$H \cdot |0\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Ceci signifie que $H \cdot |0\rangle$ donne un état qui, avec une probabilité de 50% est $|0\rangle$ et avec une probabilité de 50% est $|1\rangle$ au moment de la mesure.

Il est aussi possible d'appliquer cette porte à $|1\rangle$, ce qui donne :

$$H \cdot |1\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Remarque

$$H \cdot |0\rangle = |p\rangle, H \cdot |1\rangle = |m\rangle, H \cdot |p\rangle = |0\rangle, H \cdot |m\rangle = |1\rangle$$

Pour un état quelconque $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, l'application de la porte donne :

$$H \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$$

Interprétation géométrique

On peut montrer que $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ réalise une symétrie par rapport à la droite d'angle polaire $\frac{\pi}{8}$.

Soit $A = \begin{pmatrix} \cos(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) \end{pmatrix}$ dont l'image par une symétrie réalisée avec la droite d'angle polaire $\frac{\pi}{8}$ doit donner le point $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Effectivement,

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos(\frac{\pi}{4}) \\ \sin(\frac{\pi}{4}) \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(\frac{\pi}{4}) + \sin(\frac{\pi}{4}) \\ \cos(\frac{\pi}{4}) - \sin(\frac{\pi}{4}) \end{pmatrix} = \begin{pmatrix} 0.5 + 0.5 \\ 0.5 - 0.5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Résumé

$$H \cdot |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$H \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$$

1.1.5 Application de Hadamard sur $\mathbb{C}^q$

Il est possible d'appliquer la porte de Hadamard dans $\mathbb{C}^q$ avec $|0\rangle^q$.

$$H^{\otimes q} \cdot |0\rangle^q = (H \cdot |0\rangle)^q = \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right]^q = \frac{1}{(\sqrt{2})^q} \cdot \sum_{i=1}^{j=q} |i\rangle$$

Ainsi $H^{\otimes q}$ définit un état dans lequel tous les états possibles ont une probabilité identique.

Exemple

Considérons $H^{\otimes 2} = H \otimes H$

$$H^{\otimes 2} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H^{\otimes 2} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Donc

$$H^{\otimes 2} \cdot |00\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H^{\otimes 2} \cdot |00\rangle = \frac{1}{2} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Le résultat montre que la probabilité d'obtenir $|ij\rangle$ vaut $\frac{1}{4}$. Cette porte joue un rôle particulier car elle permet de mettre en superposition un ensemble d'états avec la même probabilité.

1.1.6 La porte quantique : X

Elle se définit par : $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

En appliquant cette porte à l'état $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, la porte inverse les deux coordonnées, ce qui donne $X \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$. Cette porte est une symétrie par rapport à la droite d'angle polaire $\frac{\pi}{4}$.

1.1.7 La porte quantique : CX

La porte CX_{ij} peut être utilisée pour faire une traduction quantique du Si ... alors ... Sinon.

L'expression matricielle de CX_{12} est :

$$CX_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Exemple d'application

$$CX_{12}|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \text{ donc } CX_{12}|11\rangle = |10\rangle$$

$$CX_{12}|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ donc } CX_{12}|10\rangle = |11\rangle$$

$$CX_{12}|01\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ donc } CX_{12}|01\rangle = |01\rangle$$

$$CX_{12}(|00\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ donc } CX_{12}(|00\rangle) = |00\rangle$$

L'expression matricielle de l'opérateur CX peut être assez complexe ou peu intuitive. Ainsi

$$CX_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Et donc

$$CX_{21}|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ donc } CX_{21}|11\rangle = |01\rangle$$

$$CX_{21}|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \text{ donc } CX_{21}|10\rangle = |10\rangle$$

$$CX_{21}|01\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ donc } CX_{21}|01\rangle = |11\rangle$$

$$CX_{21}|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ donc } CX_{21}|00\rangle = |00\rangle$$

1.1.8 La porte quantique : Z et CZ

Elle se définit par : $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

La porte CZ_{ij} consiste à appliquer la porte Z sur le qubit j si le qubit i vaut 1.

Nous avons

$$Z \cdot |0\rangle = |0\rangle$$

$$Z \cdot |1\rangle = -|1\rangle$$

Donc

$$CZ_{12}|00\rangle = |00\rangle$$

$$CZ_{12}|01\rangle = |01\rangle$$

$$CZ_{12}|10\rangle = |10\rangle$$

$$CZ_{12}|11\rangle = -|11\rangle$$

1.1.9 La porte quantique : Y et CY

Elle se définit par : $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

La porte CY_{ij} consiste à appliquer la porte Y sur le qubit j si le qubit i vaut 1.

Nous avons

$$Y \cdot |0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = i \cdot |0\rangle$$

$$Y \cdot |1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -i \cdot |1\rangle$$

Donc

$$CY_{12}|00\rangle = |00\rangle$$

$$CY_{12}|01\rangle = |01\rangle$$

$$CY_{12}|10\rangle = i \cdot |10\rangle$$

$$CY_{12}|11\rangle = -i \cdot |11\rangle$$

1.1.10 Liens entre les portes X , Y et Z

Les formules courantes sont les suivantes :

$$X \cdot Z = -i \cdot Y, \quad Z \cdot X = i \cdot Y$$

$$X \cdot Y = i \cdot Z, \quad Y \cdot X = -i \cdot Z$$

$$Y \cdot Z = i \cdot X, \quad Z \cdot Y = -i \cdot X$$

1.2 Éléments propres des portes de Pauli

On appelle vecteur propre d'un opérateur U associé à la valeur propre $\lambda \in \mathbb{C}$, tout vecteur v non nul tel que : $U \cdot v = \lambda \cdot v$

Pour les opérateurs usuels on a :

$$Z \cdot |0\rangle = |0\rangle$$

$$Z \cdot |1\rangle = -|1\rangle$$

Ce qui signifie que $|1\rangle$ est un vecteur propre de Z associé à -1 . On peut remarquer que $e^{it}|1\rangle$ est aussi un vecteur propre de Z associé à -1 .

De même on a :

$$X \cdot |p\rangle = |p\rangle$$

$$X \cdot |m\rangle = -|m\rangle$$

Avec

$$|p\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|m\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Remarque

Dans la base $B(|p\rangle, |m\rangle)$ la matrice de X est : $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}_{B(|p\rangle, |m\rangle)}$ alors que celle de Z est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{B(|p\rangle, |m\rangle)}$. Enfin la matrice de la porte de Hadamard, dans cette base, est $H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}_{B(|p\rangle, |m\rangle)}$.

De même on a :

$$Y \cdot \frac{1}{\sqrt{2}}(|0\rangle + i \cdot |1\rangle) = \left[\frac{1}{\sqrt{2}}(|0\rangle + i \cdot |1\rangle) \right]$$

$$Y \cdot \frac{1}{\sqrt{2}}(|0\rangle - i \cdot |1\rangle) = - \left[-\frac{1}{\sqrt{2}}(|0\rangle - i \cdot |1\rangle) \right]$$

Où $\frac{1}{\sqrt{2}}(|0\rangle + i \cdot |1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle - i \cdot |1\rangle)$ sont deux vecteurs propres de Y associés à 1 et -1 .

1.3 Calcul tensoriel

Soit $|\psi_1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ et $|\psi_2\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$

On note : $|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{pmatrix}$

Une notation plus compacte serait :

$$|\psi_1\rangle \otimes |\psi_2\rangle = (a \cdot |0\rangle + b \cdot |1\rangle) \otimes (c \cdot |0\rangle + d \cdot |1\rangle)$$

L'opérateur $\otimes$ étant linéaire on a :

$$|\psi_1\rangle \otimes |\psi_2\rangle = a \cdot c \cdot |00\rangle + a \cdot d \cdot |01\rangle + b \cdot c \cdot |10\rangle + b \cdot d \cdot |11\rangle$$

Ces calculs se généralisent aux opérateurs et donc aux portes quantiques.

Soit deux opérateurs :

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \text{ et } B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

Ainsi on écrit :

$$A \otimes B = \begin{pmatrix} a_1 \cdot B & a_2 \cdot B \\ a_3 \cdot B & a_4 \cdot B \end{pmatrix} = \begin{pmatrix} a_1 \cdot b_1 & a_1 \cdot b_2 & \boxed{} & \boxed{} \\ a_1 \cdot b_3 & a_1 \cdot b_4 & \boxed{} & \boxed{} \\ \boxed{} & \boxed{} & \boxed{} & \boxed{} \\ \boxed{} & \boxed{} & \boxed{} & \boxed{} \end{pmatrix}$$

Application aux portes quantiques

Considérons l'exemple de la Figure 1-1 qui définit un circuit composé de 3 portes. Si on suppose qu'on applique le circuit à l'état $|00\rangle$ on obtient :

$$|\psi\rangle = (X \otimes Id) \cdot (X \otimes Z) \cdot |00\rangle$$

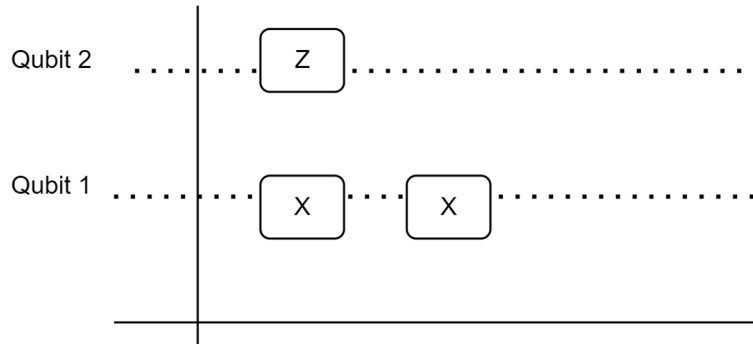


Figure 1-1. Exemple de circuit

Par convention, on peut remplacer

$$|\psi\rangle = X_1. (X_1. Z_2). |00\rangle$$

Avec la convention suivante :

A_i représente l'application de l'opérateur A sur le qubit i et l'identité sur les autres qubits.

Exemple :

Avec $n = 4$ qubits on a par exemple :

$$X_3 = Id \otimes Id \otimes X \otimes Id$$

$$Z_2 = Id \otimes Z \otimes Id \otimes Id$$

Règles de calcul

Si $|\psi\rangle$, $|\phi\rangle$ et $|\sigma\rangle$ sont des qubits et si z est un complexe, alors

$$(|\psi\rangle + |\phi\rangle) \otimes |\sigma\rangle = (|\psi\rangle \otimes |\sigma\rangle) + (|\phi\rangle \otimes |\sigma\rangle)$$

$$|\sigma\rangle \otimes (|\psi\rangle + |\phi\rangle) = (|\sigma\rangle \otimes |\psi\rangle) + (|\sigma\rangle \otimes |\phi\rangle)$$

$$z. (|\psi\rangle \otimes |\phi\rangle) = (z. |\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (z. |\phi\rangle)$$

Attention, en général, $(|\psi\rangle \otimes |\phi\rangle) \neq (|\phi\rangle \otimes |\psi\rangle)$.

Si A et B sont des opérateurs linéaires sur un qubit, alors

$$(A \otimes B). (|\psi\rangle \otimes |\phi\rangle) = (A. |\psi\rangle) \otimes (B. |\phi\rangle)$$

1.4 Exponentielle

Si $U \in SU(2)$ c'est-à-dire que $U^2 = Id$ alors :

$$\begin{aligned}
 e^{i.t.U} &= \sum_{k=0}^{\infty} \frac{(i.t.U)^k}{k!} = \sum_{k=0}^{\infty} \frac{(i.t.U)^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{(i.t.U)^{2k+1}}{(2k+1)!} \\
 e^{i.t.U} &= \sum_{k=0}^{\infty} \frac{(i.t)^{2k}}{(2k)!} \cdot U^{2k} + \sum_{k=0}^{\infty} \frac{(i.t)^{2k+1}}{(2k+1)!} \cdot U^{2k+1} \\
 e^{i.t.U} &= \sum_{k=0}^{\infty} \frac{(-1)^k \cdot t^{2k}}{(2k)!} \cdot Id + \sum_{k=0}^{\infty} \frac{i \cdot (-1)^k \cdot t^{2k+1}}{(2k+1)!} \cdot U
 \end{aligned}$$

donc

$$e^{i.t.U} = \cos t \cdot Id + i \cdot \sin t \cdot U$$

Exemple :

$$e^{i.t.X} = \cos t \cdot Id + i \cdot \sin t \cdot X$$

Donc

$$e^{i.t.X} \cdot |0\rangle = \cos t \cdot |0\rangle + i \cdot \sin t \cdot X \cdot |0\rangle$$

$$e^{i.t.X} \cdot |0\rangle = \cos t \cdot |0\rangle + i \cdot \sin t \cdot |1\rangle$$

1.5 Notion d'Hamiltonien

On appelle Hamiltonien un opérateur particulier composé de portes Z_i et de tous les opérateurs obtenus par multiplication de ces opérateurs. Ainsi les expressions suivantes

$$Z_1, Z_2 \dots Z_n \text{ et } Z_1 \cdot Z_2$$

correspondent à des Hamiltoniens. De manière générale les hamiltoniens considérés sont de la forme :

$$H = \alpha \cdot Z_1 + \beta \cdot Z_2 + \gamma \cdot Z_1 \cdot Z_2 \dots$$

Un Hamiltonien H représente une fonction f si les plus petites valeurs propres de H correspondent aux solutions qui minimisent f .

Exemple

Soit $(1 - q_1) \cdot (1 - q_2) = 1$

La fonction $1 - (1 - q_1) \cdot (1 - q_2)$ est minimale lorsque $q_1 = q_2 = 0$.

L'Hamiltonien

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

"représente" la fonction f car la plus petite valeur propre de H vaut 0 et correspond à la colonne $|00\rangle$.

Pour transformer une expression usuelle en Hamiltonien il faut remplacer les variables usuelles par

$$\frac{1}{2}(Id - Z_1) \text{ ou } \frac{1}{2}(Id + Z_1)$$

Selon les cas.

Les règles à appliquer.**Règle 1.**

Si l'expression initiale implique que $q_1 = 0$, il s'agit de remplacer q_1 par :

$$\frac{1}{2}(Id - Z_1) = \begin{pmatrix} 0 & \square \\ \square & 1 \end{pmatrix}$$

puisque la plus petite valeur propre de $\frac{1}{2}(Id - Z_1)$ correspond à $|0\rangle$.

Règle 2.

Si l'expression initiale implique que $q_1 = 1$, il s'agit de remplacer q_1 par :

$$\frac{1}{2}(Id + Z_1) = \begin{pmatrix} 1 & \square \\ \square & 0 \end{pmatrix}$$

puisque la plus petite valeur propre de $\frac{1}{2}(Id + Z_1)$ correspond à $|1\rangle$.

Règle 3.

Dans le cas d'un ET dans une expression logique il s'agit d'additionner les Hamiltoniens.

Exemple

$$(1 - q_1) \cdot (1 - q_2) = 1$$

correspond à

$$H = \frac{1}{2}(Id + Z_1) + \frac{1}{2}(Id + Z_2)$$

$$H = Id + \frac{1}{2}Z_1 + \frac{1}{2}Z_2$$

On peut facilement vérifier la modélisation en considérant les expressions matricielles des portes.

Ainsi

$$Id = \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & 1 \end{pmatrix}$$

$$Z_1 = Z \otimes Id = \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & -1 \end{pmatrix}$$

$$Z_2 = Id \otimes Z = \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & -1 \end{pmatrix}$$

$$Z_1 \cdot Z_2 = \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & -1 \end{pmatrix} = \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & 1 \end{pmatrix}$$

Donc

$$H = Id + \frac{1}{2}Z_1 + \frac{1}{2}Z_2$$

$$H = \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & 1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & -1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & -1 \end{pmatrix}$$

$$H = \begin{pmatrix} 2 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & 0 \end{pmatrix}$$

Remarque

L'expression

$$(1 - q_1) \cdot (1 - q_2) = 1$$

peut s'analyser sur un plan logique.

Cela consiste à marquer les états tels que au moins une variable vaille 0 (donc 00, 01 et 10) et pour cela il faut utiliser $\frac{1}{2}(Id - Z_1)$ avec une multiplication par $\frac{1}{2}(Id - Z_2)$ car la multiplication représente un "ou" logique. Une fois obtenu l'hamiltonien on "inverse" le résultat en faisant un Id moins cet hamiltonien de sorte qu'on marque les états n'ayant que des 1.

Donc

$$H = Id - \frac{1}{2}(Id - Z_1) \cdot \frac{1}{2}(Id - Z_2)$$

est l'hamiltonien associé.

Car

$$\begin{aligned} \frac{1}{2}(Id - Z_1) \cdot \frac{1}{2}(Id - Z_2) &= \frac{1}{4}(Id - Z_1 - Z_2 + Z_1 Z_2) \\ \frac{1}{2}(Id - Z_1) \cdot \frac{1}{2}(Id - Z_2) &= \frac{1}{4} \left[\begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & 1 \end{pmatrix} - \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & -1 \end{pmatrix} \right. \\ &\quad \left. - \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & -1 \end{pmatrix} + \begin{pmatrix} 1 & \square & \square & \square \\ \square & -1 & \square & \square \\ \square & \square & -1 & \square \\ \square & \square & \square & 1 \end{pmatrix} \right] \end{aligned}$$

$$\frac{1}{2}(Id - Z_1) \cdot \frac{1}{2}(Id - Z_2) = \begin{pmatrix} 0 & \square & \square & \square \\ \square & 0 & \square & \square \\ \square & \square & 0 & \square \\ \square & \square & \square & 1 \end{pmatrix}$$

On constate qu'on a "marqué" les colonnes ayant au moins une valeur 0 soit $|00\rangle$, $|01\rangle$ et $|10\rangle$.

Donc

$$Id - \frac{1}{2}(Id - Z_1) \cdot \frac{1}{2}(Id - Z_2) = \begin{pmatrix} 1 & \square & \square & \square \\ \square & 1 & \square & \square \\ \square & \square & 1 & \square \\ \square & \square & \square & 0 \end{pmatrix}$$

1.6 Méta-Heuristiques Quantiques

1.6.1 Résolution approchée de l'équation de Schrödinger

Dans le cas général, la solution de l'équation de Schrödinger est :

$$|\psi_T\rangle = e^{-\frac{i}{\hbar} \int_0^T H(u) du} \cdot |\psi_0\rangle$$

La résolution directe de cette équation est dans la majorité des cas impossibles, mais les résolutions approchées restent possibles car l'intervalle de temps $[0; T]$ peut être découpé en n intervalles plus petits de longueur $\Delta t = \frac{T}{n}$ tels que, sur ces intervalles de longueur Δt , $|\psi_t\rangle$ puisse être considéré comme indépendant du temps.

Donc :

$$|\psi_T\rangle = e^{-\frac{i}{\hbar} \int_0^T H(u) du} \cdot |\psi_0\rangle$$

$$|\psi_T\rangle = e^{-\frac{i}{\hbar} \sum_{k=0}^{n-1} \int_{k\Delta t}^{(k+1)\Delta t} H(u) du} \cdot |\psi_0\rangle$$

Comme $e^{i.(A+B).t} \approx e^{i.(A).t} \cdot e^{i.(B).t}$ il vient :

$$|\psi_T\rangle \simeq e^{-\frac{i}{\hbar} \int_{(n-1)\Delta t}^{n\Delta t} H(u) du} \dots e^{-\frac{i}{\hbar} \int_{\Delta t}^{2\Delta t} H(u) du} \cdot e^{-\frac{i}{\hbar} \int_0^{\Delta t} H(u) du} |\psi_0\rangle$$

Ceci est un résultat très important car il prouve qu'on peut avoir une approximation de la solution en considérant que sur chaque intervalle, si Δt est suffisamment petit, on a :

$$|\psi_{t+\Delta t}\rangle = e^{-\frac{i}{\hbar} \Delta t \cdot H(t)} |\psi_t\rangle$$

1.6.2 Principes de l'algorithme adiabatique

Dans le cas d'un algorithme itératif, à l'itération k , cela donne le calcul suivant :

$$|\psi_{k+1}\rangle = e^{-\frac{i}{\hbar}\Delta t.H(k.\Delta t)}|\psi_k\rangle$$

Et on peut définir l'état initial par

$$|\psi_0\rangle = |p\rangle^{\otimes n} = |+\rangle^{\otimes n}$$

Il s'agit ensuite de considérer des Hamiltoniens particuliers (Farhi *et al.*, 2000) (Farhi *et al.*, 2002) et (Farhi *et al.*, 2014) de la forme :

$$H(t) = t.H_p + (1 - t).H_D$$

Ces Hamiltoniens permettent de passer de H_D l'Hamiltonien initial à l'Hamiltonien H_p qui correspond à l'Hamiltonien du problème à résoudre.

Dans le cas particulier de l'**optimisation adiabatique**, il suffit de choisir :

$$H(t) = s(t).H_D + [1 - s(t)].H_p$$

avec $s(t) = 1 - t.\Delta t$ et $\Delta t = \frac{1}{n}$ où n est le nombre de découpages de l'intégrale utilisée pour faire l'approximation. On obtient ainsi un processus durant lequel le poids relatif de H_D et H_p évolue lentement et passe de H_D à H_p progressivement. Ceci est représenté sur la Figure 1-2.

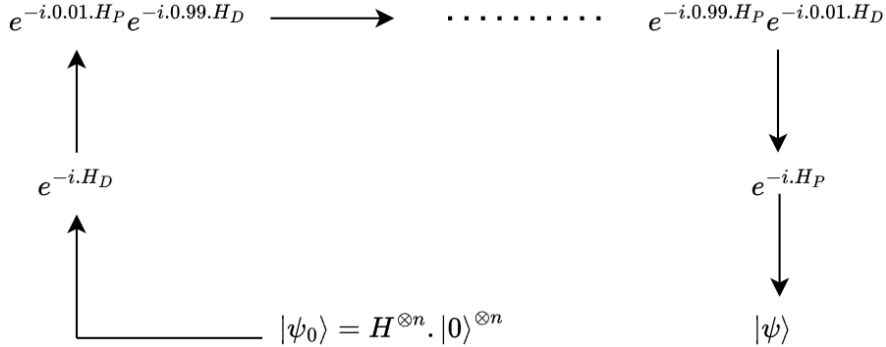


Figure 1-2. Visualisation d'un Hamiltonien adiabatique

L'utilisation d'une méthode adiabatique aboutit à la des circuits de grande taille à cause de la nécessité de définir Δt petit afin que l'approximation de l'intégrale soit de bonne qualité. Pour contourner cette limitation plusieurs méthodes ont été développées et la plus connue est certainement la méthode QAOA. L'idée est simple : il s'agit de considérer que chaque état se définit par des angles dans la sphère de Bloch. Comme les exponentielles utilisées donnent des circuits composés de rotations, il s'agit simplement de paramétrer ces rotations.

Ainsi on définit $H = H_D(\beta) + H_P(\gamma)$ qui dépend des angles β et γ .

Pour obtenir une précision suffisante, on peut alterner plusieurs fois H_D/H_P ce qui est défini par le paramètre p appelé "profondeur".

$$e^{-i.H_D(\gamma_p)}.e^{-i.H_P(\beta_p)}.e^{-i.H_D(\gamma_{p-1})}.e^{-i.H_P(\beta_{p-1})} \dots e^{-i.H_D(\gamma_1)}.e^{-i.H_P(\beta_1)}$$

A chaque choix d'angle on peut associer un coût moyen $\langle s | e^{-i.H_P(\beta, \gamma)} | s \rangle$ et rechercher, en faisant varier les angles la solution associée au coût moyen minimal. Une méthode de minimisation telle que Cobyla peut parcourir l'ensemble des Hamiltoniens et rechercher les angles $\vec{\beta}^*, \vec{\gamma}^*$ qui définissent l'Hamiltonien de coût minimal.

Pour que cet algorithme soit efficace en pratique, d'une part il doit nécessiter un nombre raisonnable de tirages pour évaluer la moyenne et, d'autre part, il faut que la distribution de probabilité, au cours des itérations, s'agrège autour des "bonnes solutions".

1.7 Conclusion

Ce chapitre est une introduction aux notions fondamentales utiles en quantique et qui sont utilisées par la suite.

1.8 Références

E. Bourreau, G. Fleury et P. Lacomme. *Introduction à l'informatique quantique*. Eyrolles. 2022.

E. Farhi, J. Goldstone, S. Gutmann and M. Sipser, Quantum Computation by Adiabatic Evolution, *Quantum Physics (quant-ph)*, [arXiv:quant-ph/0001106](https://arxiv.org/abs/quant-ph/0001106), 2000.

E. Farhi, J. Goldstone and S. Gutmann, Quantum Adiabatic Evolution Algorithms versus Simulated Annealing, *Quantum Physics (quant-ph)*, [arXiv:quant-ph/0201031](https://arxiv.org/abs/quant-ph/0201031), 2002.

E. Farhi and J. Goldstone, A Quantum Approximate Optimization Algorithm, *Quantum Physics (quant-ph)*, [arXiv:1411.4028](https://arxiv.org/abs/1411.4028), 2014.

CHAPITRE 2

Algorithme d'Estimation de la Phase (QPE)

Objectifs : l'algorithme d'estimation de la phase (en anglais QPE pour Quantum Phase Estimation) a été proposé en 1995 par Alexei Kitaev. Son objectif est d'associer à un vecteur propre d'un opérateur unitaire, sa valeur propre qui peut être lue à la sortie du circuit sous la forme d'une phase. Dans sa forme originale, le circuit nécessite de connaître un vecteur propre d'une part et d'autre part d'être capable d'exprimer l'opérateur unitaire. Le principe de cet algorithme est illustré sur un TSP (Traveling Salesman Problem) de 4 sommets dans le chapitre 3.

2.1 Quantum Phase Estimation (QPE) : présentation

2.1.1 Définition

On considère le circuit de la Figure 2-1 avec p qubits utilisés pour représenter la phase et n qubits pour représenter un vecteur propre. Ce circuit a été proposé pour la première fois en 1995 par Kitaev (Kitaev, 1995).

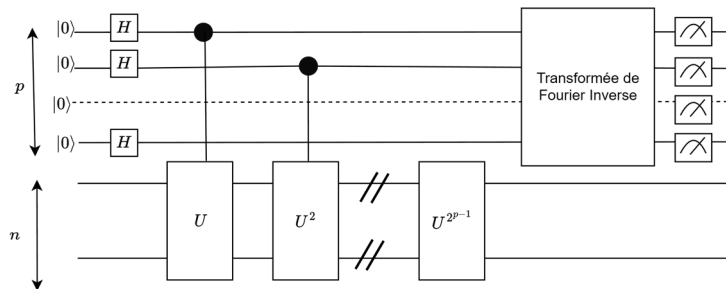


Figure 2-1. Circuit pour QPE

L'objectif de l'algorithme est, connaissant un vecteur propre de l'opérateur U , de lui associer la valeur propre correspondante. Cet algorithme ne s'applique qu'à un

opérateur U unitaire (i.e. $U.U^\dagger = Id$). On note μ la valeur propre associée à un vecteur propre $|\psi\rangle$.

Remarque

$$\langle x|\mu.\mu^*|x\rangle = \langle x|U.U^\dagger|x\rangle = \langle x|x\rangle$$

Donc $|\mu| = 1$

Il est donc possible d'écrire que $\mu = e^{2\pi.i.\theta}$ où $\theta \in [0; 1[$.

On suppose alors que $\theta = \sum_{k=1}^n \theta_k . 2^{-k}$ avec $\theta_k \in \{0; 1\}$.

Dans le cas particulier où l'on s'intéresse seulement à 2 qubits le circuit se simplifie et la transformée de Fourier se réduit à une porte de Hadamard (Kitaev, 1995) comme le montre la Figure 2-2.

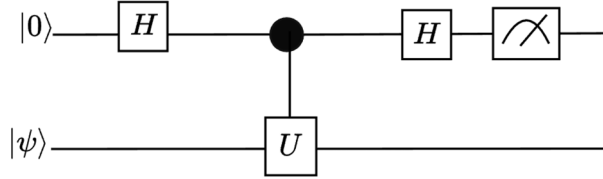


Figure 2-2. Circuit pour QPE avec 1 qubit pour la valeur propre et un qubit pour le vecteur propre $|\psi\rangle$

2.1.2 Un seul qubit de contrôle

En supposant que l'opérateur U est unitaire, on suppose donc les N valeurs propres de U peuvent toutes s'écrire comme :

$$\mu_1 = e^{2\pi.i.\theta_1}$$

...

$$\mu_N = e^{2\pi.i.\theta_N}$$

Ainsi dans la base des vecteurs propres de U , en notant $|\psi_k\rangle$ le vecteur propre numéro k , nous avons :

$$U = \sum_{k=1}^N \mu_k . |\psi_k\rangle\langle\psi_k|$$

Donc dans la base des vecteurs propres :

$$U . |\psi_k\rangle = \mu_k . |\psi_k\rangle$$

$$U . |\psi_k\rangle = e^{2\pi.i.\theta_k} . |\psi_k\rangle$$

De manière générique on écrit :

$$U.|\psi\rangle = e^{2\pi.i.\theta}.|\psi\rangle$$

Avec $\theta \in [0; 1[$

Supposons alors que $\theta \simeq \frac{y}{2^p}$ avec $y \in \{0; 1; 2; \dots; 2^{p-1}\}$

Analysons le circuit de la Figure 2-2.

Étape 0.

L'état initial est, dans le cas particulier de deux qubits :

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle)$$

Étape 1. Elle consiste à appliquer le CU

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U.|\psi\rangle)$$

Si $|\psi\rangle$ est un vecteur propre de U alors : $U.|\psi\rangle = e^{2\pi.i.\theta}.|\psi\rangle$

donc

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes e^{2\pi.i.\theta}.|\psi\rangle)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi.i.\theta}.|1\rangle) \otimes |\psi\rangle$$

Étape 2. Il s'agit d'appliquer H au premier qubit.

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}H.(|0\rangle + e^{2\pi.i.\theta}.|1\rangle) \otimes |\psi\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(H.|0\rangle + e^{2\pi.i.\theta}.H.|1\rangle) \otimes |\psi\rangle$$

Or

$$H.|0\rangle = \frac{1}{\sqrt{2}}.(|0\rangle + |1\rangle)$$

$$H. |1\rangle = \frac{1}{\sqrt{2}}. (|0\rangle - |1\rangle)$$

Donc

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}}. (|0\rangle + |1\rangle) + e^{2\pi.i.\theta}. \frac{1}{\sqrt{2}}. (|0\rangle - |1\rangle) \right) \otimes |\psi\rangle$$

$$|\psi_2\rangle = \frac{1}{2} \left((|0\rangle + |1\rangle) + e^{2\pi.i.\theta}. (|0\rangle - |1\rangle) \right) \otimes |\psi\rangle$$

$$|\psi_2\rangle = \left(\frac{1 + e^{2\pi.i.\theta}}{2} |0\rangle + \frac{1 - e^{2\pi.i.\theta}}{2} |1\rangle \right) \otimes |\psi\rangle$$

Étape 3. Réalisation d'une mesure

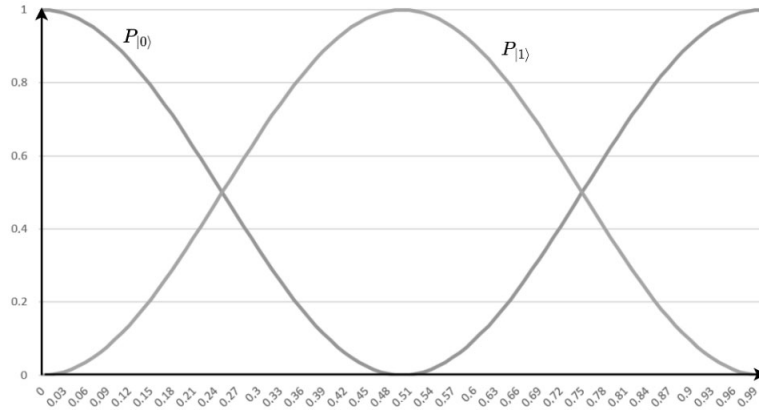
En réalisant la mesure sur le qubit 1, nous pouvons calculer $P_{|0\rangle}$ la probabilité d'obtenir $|0\rangle$ et $P_{|1\rangle}$ la probabilité d'obtenir $|1\rangle$.

$$\begin{aligned} P_{|0\rangle} &= \left| \frac{1 + e^{2\pi.i.\theta}}{2} \right|^2 = \left| \frac{1 + \cos 2\pi.\theta + i.\sin 2\pi.\theta}{2} \right|^2 \\ &= \left| \frac{1 + \cos 2\pi.\theta}{2} + \frac{\sin 2\pi.\theta}{2} i \right|^2 \\ P_{|0\rangle} &= \left(\frac{1 + \cos 2\pi.\theta}{2} \right)^2 + \left(\frac{\sin 2\pi.\theta}{2} \right)^2 \\ P_{|0\rangle} &= \frac{1 + 2.\cos 2\pi.\theta + \cos^2 2\pi.\theta}{4} + \frac{\sin^2 2\pi.\theta}{4} \\ P_{|0\rangle} &= \frac{2 + 2.\cos 2\pi.\theta}{4} = \frac{1 + \cos 2\pi.\theta}{2} = \cos^2 \pi.\theta \end{aligned}$$

Et par conséquent

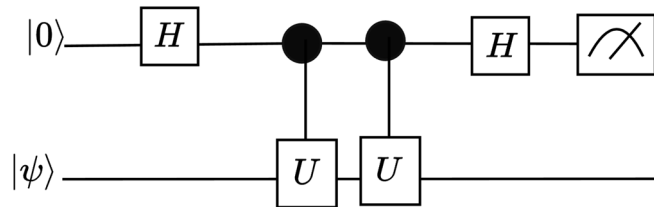
$$P_{|1\rangle} = \left| \frac{1 - e^{2\pi.i.\theta}}{2} \right|^2 = \sin^2 \pi.\theta$$

L'évolution de ces deux probabilités est donnée sur la Figure 2-3.


 Figure 2-3. Evolution des deux probabilités en fonction de θ

2.1.3 Application de deux fois U et un seul qubit de contrôle

Il est possible d'analyser ce que représente l'application successive de deux portes U ce qui correspondrait au schéma de la Figure 2-4.


 Figure 2-4. Circuit pour QPE et 2 fois la porte U et avec 2 qubits et un vecteur propre $|\psi\rangle$

Étape 0.

L'état initial est dans le cas particulier de deux qubits :

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle)$$

Étape 1. Elle consiste à appliquer le premier CU

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U \cdot |\psi\rangle)$$

Si $|\psi\rangle$ est un vecteur propre de U alors : $U \cdot |\psi\rangle = e^{2\pi i \theta} \cdot |\psi\rangle$

donc