Introduction à l'informatique quantique

Philippe DENIEL (philippe.deniel@cea.fr)

CEA / ENSIEE

2024

Introduction

De quoi va-t-on parler pendant ces 42 heures de cours ?

Plan

1 Qu'est-ce que l'informatique quantique

Quelques citations

Niels Bohr - Si la mécanique quantique ne vous a pas encore profondément choqué, alors vous ne l'avez pas encore comprise. Tout ce que nous appelons réel est fait de choses qui ne peuvent pas être considérées comme étant réelles.

Niels Bohr - Si une idée ne semble pas bizarre, il n'y a rien à espérer d'elle.

Heinz Pagels - Dieu a utilisé de merveilleuses mathématiques pour créer le monde.

Richard Feynmann - Je pense pouvoir dire sans trop me tromper que personne ne comprend la mécanique quantique.

Richard Feynmann, 1982 - Nature isn't classical, dammit, and if you want to make a simulation of nature, you better make it quantum mechanical

Albert Einstein - If you can't explain it simply, you don't understand it well enough

L'informatique quantique n'est pas si récente

Le *Quentum Computing* est né dans les années 80

- Une première conférence sur le QC au MIT en 1981
- Beaucoup d'études théoriques sur le QC
  - Algorithme de Shor, 1994
  - Algorithme de Grover, 1996

L'informatique quantique a de solides bases théoriques

- dans le domaine de la physique (physique quantique, physique statistique)
- dans le domaine des mathématiques (algèbre linéaire, algèbre hermitienne)

En revanche les implémentations physiques "réelles" des QPUs sont très récents.

Les liens entre informatique quantique et physique quantique

Le *Quantum Computing* est un nouveau paradigme informatique basé sur les phénomènes à la physique quantique :

1. la superposition,
   - qui permet d'induire une forme de parallélisme (à relativiser...)
2. l'intrication,
   - qui permet de coupler des systèmes simples pour de bâtir des systèmes plus complexes
3. les interférences,
   - qui permettent de mesurer les états quantiques et d'obtenir des résultats de calcul.

La première révolution quantique

La physique quantique est déjà très présente dans notre monde

- imagerie médicale : IRM (imagerie par résonance magnétique,
- composants électroniques : transistors à effet tunnel, LED,
- lasers,
- écrans LCD,
- panneaux solaires photovoltaïques : interaction photon/matière.

7 / 370

Le QC et la deuxième révolution quantique

L'informatique quantique fait partie de la deuxième révolution quantique

Les **QPU** commencent à apparaître sur le marché.

On prévoit plusieurs phases dans le QC

- NISQ : **N**oisy **I**ntermediate **S**cale **Q**uantum
- FTQC : **F**ault **T**olerant **Q**uantum **Q**uantum
- LSQ : **L**arge **S**cale **Q**uantum

On est actuellement dans la période NISQ

Ce que l'informatique quantique n'est pas.

Le QC ne va pas remplacer le HPC

- Les QPUs appartiennent à un nouveau paradigme du HPC, comme les GPUs.
- le QC est une nouvelle arme dans l'arsenal du HPC

Attention à la "hype" autour du QC, entretenue par certains constructeurs (dont IBM et Google)

- Des annonces "publicitaires", parfois éloignées de la réalité scientifique
- Des notions "grand public" aux contours souvent très flous...
- le QC ce n'est pas "faire 2^n calculs en même temps", le parallélisme exponentiel existe mais il est loin d'être systématique
- le QC est efficace pour caractériser rapidement une propriété globale d'un problème
  - périodicité d'une fonction entière (Shor)
  - parcours de graphe (marches quantiques)
  - Recherches d'optima de forme quadratiques (QUBO)

9 / 370

Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

Les espaces de Hilbert

Un espace de Hilbert est un espace vectoriel sur les corps $\mathbb{R}$ ou $\mathbb{C}$ qui dispose des propriétés suivantes :

- il est euclien ou hermitien, c'est à dire qu'il dispose d'un produit scalaire (euclidien si basé sur $\mathbb{R}$, hermitien si base sur $\mathbb{C}$), ce dernier permet de définir une distance, mais aussi des notions d'angles et d'orthogonalité ;
- il est *complet*.

Dans un espace vectoriel *complet*, les suites de Cauchy convergent.

Suites de Cauchy

Les suites de Cauchy désignent les suites $(u_n)_{n\in\mathbb{N}}$ qui vérifient la propriété suivante (La fonction $d()$ désigne ici la distance dans l'espace de Hilbert) :

$$\lim_{p,q\to+\infty} d(r_p, r_q) = 0$$

Intuitivement, une suite de Cauchy est une suite dont les termes se rapprochent de plus en plus quant l'indice de la suite augmente. On a un espace de Hilbert quand ces suites convergent vers une valeur qui est dans l'espace en question.
En bref, un espace de Hilbert, c'est un espace vectoriel qui contient tous les "outils" mathématiques dont on a besoin pour y faire de l'analyse.

Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

Rappels : les matrices

Une matrice à m lignes et n colonnes dont chaque case prend sa valeur dans un corps $\mathbb{K}$.
Dans le périmètre de ce cours, le corps en question sera toujours le corps des nombres complexes $\mathbb{C}$
On notera les éléments $a_{i,j}$ d'une matrice $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$ soit encore

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

Rappels : matrices transposées et adjointes

La transposée d'une matrice A de taille m.n est notée A^t, c'est une matrice de taille n.m telle que

$$A' = (a'_{i,j})_{1\leq i\leq n, 1\leq j\leq m} = A^t, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = a_{i,j}$$

La matrice adjoite d'une matrice A de taille m.n est notée A^*, c'est une matrice de taille n.m telle que

$$A' = (a'_{i,j})_{1\leq i\leq n, 1\leq j\leq m} = A^*, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = \overline{a_{i,j}}$$

Matrice Adjointe = transposée + conjugaison

Rappels : trace d'une matrice

La trace d'une matrice carrée est une fonction qui associe à une matrice la somme des éléments sur sa diagonale. En termes mathématiques, on écrira

$$A = (a_{ij})_{1 \leq i,j \leq n}, Tr(A) = \sum_{i=1}^{n} a_{ii}$$

La trace possède différentes propriétés remarquables :

$$\begin{aligned} Tr(A + B) &= Tr(A) + Tr(B) \\ Tr(\alpha A) &= \alpha Tr(A) \\ Tr(A^t) &= Tr(A) \\ Tr(AB) &= Tr(BA) \end{aligned}$$

La trace est un *invariant de similitude*

$$Tr(PAP^{-1}) = Tr(APP^{-1}) = Tr(A)$$

Produit matriciel (usuel)

Le produit matriciel est plus complexe. Le produit est non-commutatif et il impose que le nombre de colonnes de l'élément de gauche est égale au nombre de lignes de l'élément de droite, on ne pourra donc former le produit $A \times B$ que si A est une matrice de taille $m \times n$ et B une matrice de taille $n \times p$. Le résultat est une matrice de taille $m \times p$.
Si $a_{i,j}$, $b_{i,j}$ et $c_{i,j}$, sont les coefficients des matrices A, B et C, le produit sera défini par

$$\forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq p, c_{i,j} = \sum_{k=1}^{n} a_{i,k}.b_{k,j}$$

Le produit matriciel standard n'est pas commutatif, il est associatif et distributif à droite et à gauche par rapport à la somme.

Produit de Kronecker 1/2

Le produit de Kronecker, ou produit tensoriel est très intuitif. Il n'est pas commutatif et peut agir sur tout couple de matrices, quelque soit leurs taillse.
Si $A = (a_{ij})$ est une matrice $m \times n$ et B une matrice $p \times q$, le produit $C = A \otimes B$ sera une matrice de taille $mp \times nq$

$$A_{m,n} \otimes B_{p,q} = C_{mp,nq} = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{pmatrix}$$

Produit de Kronecker 2/2

Ce qui revient à écrire :

$$A_{m,n} \otimes B_{p,q} = \begin{pmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & \cdots & a_{1,1}b_{1,q} & \cdots & \cdots & a_{1,n}b_{1,1} & a_{1,n}b_{1,2} & \cdots & a_{1,n}b_{1,q} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & \cdots & a_{1,1}b_{2,q} & \cdots & \cdots & a_{1,n}b_{2,1} & a_{1,n}b_{2,2} & \cdots & a_{1,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{1,1}b_{p,1} & a_{1,1}b_{p,2} & \cdots & a_{1,1}b_{p,q} & \cdots & \cdots & a_{1,n}b_{p,1} & a_{1,n}b_{p,2} & \cdots & a_{1,n}b_{p,q} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{1,1} & a_{m,1}b_{1,2} & \cdots & a_{m,1}b_{1,q} & \cdots & \cdots & a_{m,n}b_{1,1} & a_{m,n}b_{1,2} & \cdots & a_{m,n}b_{1,q} \\ a_{m,1}b_{2,1} & a_{m,1}b_{2,2} & \cdots & a_{m,1}b_{2,q} & \cdots & \cdots & a_{m,n}b_{2,1} & a_{m,n}b_{2,2} & \cdots & a_{m,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{p,1} & a_{m,1}b_{p,2} & \cdots & a_{m,1}b_{p,q} & \cdots & \cdots & a_{m,n}b_{p,1} & a_{m,n}b_{p,2} & \cdots & a_{m,n}b_{p,q} \end{pmatrix}$$

Exemple de produit tensoriel

Par exemple :

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 2 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \\ 3 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 0 & 1 \times 3 & 2 \times 0 & 2 \times 3 \\ 1 \times 2 & 1 \times 1 & 2 \times 2 & 2 \times 1 \\ 3 \times 0 & 3 \times 3 & 1 \times 0 & 1 \times 3 \\ 3 \times 2 & 3 \times 1 & 1 \times 2 & 1 \times 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 3 & 0 & 6 \\ 2 & 1 & 4 & 2 \\ 0 & 9 & 0 & 3 \\ 6 & 3 & 2 & 1 \end{pmatrix}$$

Propriétés importantes du produit tensoriel

Le produit tensoriel a des propriétés notables vis-à-vis du produit matriciel classique et de la transposition :

$$(A \otimes B) \times (C \otimes D) = (A \times C) \otimes (B \times D)$$

$$(A \otimes B)^t = A^t \otimes B^t$$

Produit tensoriel d'espaces vectoriel - définition

Le produit tensoriel de matrice est intimement lié à une autre notion, celle de produit tensoriel d'espaces vectoriels. D'une manière très intuitive, un groupe ou un espace vectoriel sont des ensembles qui possèdent certaines structures qui leur donnent des propriétés intéressantes.

Si je dispose de deux ensemble A et B, je peux construire leur produit cartésien $A \times B$ dont les éléments seront des couples de la forme (x, y) avec $x \in A$ et $y \in B$. Le produit tensoriel, en approche simplifiée, permet de conserver les structures intéressantes des groupes ou des espaces vectoriels dans le produit cartésien.

Dans le cas des espaces vectoriels relatifs à un corps commutatif $\mathbb{K}$, on définira le produit tensoriel de deux espaces vectoriels E et F par l'existence d'une application bilinéaire Φ telle que :

$$\Phi : E \times F \longrightarrow E \otimes F$$

Les éléments de $E \otimes F$ sont définis par Φ en posant

$$\forall x \in E, \forall y \in F, x \otimes y = \Phi(x, y)$$

Produit tensoriel d'espace vectoriel - comment s'en servir ?

Le produit tensoriel peut être vue comme une astuce de notation car il permet de gérer des applications multilinéaires comme s'il s'agissait d'une application linéaire appliquée sur le produit tensoriel des espaces vectoriels source.

Considérons par exemple l'application bilinéaire g opérant sur $E \times F$, on peut lui adjoindre une unique forme linéaire$\hat{g}$ telle que $g = \hat{g} \circ \Phi$, où Φ représente l'isomorphisme entre $E \times F$ et $E \otimes F$. On a donc

$$\forall x \in E, \forall y \in F, g(x, y) = \hat{g}(x \otimes y)$$

On peut substituer à g, qui est bilinéaire, $\hat{g}$ qui est simplement linéaire. Grâce au produit tensoriel d'espaces vectoriels, traiter des formes multilinéaires revient à traiter de simples formes linéaires.

La dimension de l'espace produit tensoriel $E \otimes F$ est égal au produit des dimensions de E et F :

$$dim(E \otimes F) = dim(E).dim(F)$$

Retour sur le produit de Kronecker

Le lien entre le produit tensoriel d'espaces vectoriels et le produit tensoriel de matrices est canonique. En effet, connaissant une application linéaire sur E décrite par la matrice A, et une application linéaire décrite par la matrice B, je peux construire une application linéaire $A \otimes B$ sur $E \otimes F$ avec le produit de Kronecker.

La notation de produit tensoriel est très utilisée en informatique quantique. Elle servira beaucoup quand il s'agira de gérer de multiples qubits.

Attention : la notation $\otimes$ qui représente le produit tensoriel ne doit pas être confondue avec la notation $\oplus$ qui représente le XOR booléen ou la *somme directe* d'espace vectoriel.

Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

Rappels - Série de Taylor 1/2

On rappelle que la fonction exponentielle peut s'écrire comme la série suivante (série de Taylor de la fonction exponentielle) :

$$\forall x \in \mathbb{R}, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

Application à la trigonométrie
Si on y applique la série précédente à la forme $e^{i\theta}$:

$$\begin{aligned} e^{i\theta} = \sum_{n=0}^{+\infty} \frac{(i\theta)^n}{n!} &= \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p}}{2p!} + \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p+1}}{2p+1!} \\ &= \sum_{p=0}^{+\infty} \frac{(-1)^p.\theta^{2n}}{2p!} + i.\sum_{p=0}^{+\infty} \frac{(-1)^n\theta^{2p+1}}{2p+1!} \\ &= cos((\theta) + i.sin(\theta) \end{aligned}$$

Rappels - Série de Taylor 2/2

Par conséquent on peut en déduire les développements en série de Taylor des fonctions sinus et cosinus :

$$cos(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^2 n}{(2n)!}$$

$$sin(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

Exponentielle de matrices

Comme on sait multiplier des matrices carrées et les ajouter, il est possible d'utiliser la série de Taylor de l'exponentielle sur les matrices carrées. On aura donc la définition suivante :

$$\forall A \text{ matrice carrée}, e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$$

Exponentielles de matrice et valeurs propres

Les valeurs propres d'une exponentielle de matrice sont les exponentielles des valeurs propres. Ce résultat est simple à voir. En effet, si D désigne la matrice diagonale dont les coefficients sont les valeurs propres, on a trivialement

$$\exists P, A = PDP^{-1}, \forall n \in \mathbb{N}, A^n = PD^nP^{-1}$$

Par conséquent,

$$e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!} = \sum_{n=0}^{+\infty} \frac{PD^nP^{-1}}{n!} = P(\sum_{n=0}^{+\infty} \frac{D^n}{n!})P^{-1} = P.e^D.P{-}1$$

On en déduit qu'une matrice et son exponentielle ont les mêmes vecteurs propres (et par ailleurs les mêmes vecteurs propres que toutes ses puissances).

ATTENTION A LA COMMUTATIVITÉ !!!!!!!

L'exponentielle de la somme de deux matrices n'estle produit des exponentielles des matrices que si celles-ci commutent.

$$\text{En général } e^{A+B} \neq e^{A}.e^{B} \text{ , ce n'est vrai que si } AB = BA$$

Plus généralement, on dispose de la formule de *Glauber*

$$e^{X}e^{Y} = e^{X+Y+\frac{1}{2}[X,Y]}$$

Où $[X, Y]$ est le commutateur $[X, Y] = XY - YX$

Propriétés des exponentielles de matrices

L'exponentielle de la matrice nulle est la matrice identité : $e^0 = I$

Le déterminant de l'exponentielle d'une matrice est égal à l'exponentielle de sa trace :

$$det(e^X) = e^{Tr(X)}$$

Si Y est une matrice inversible alors

$$e^{YXY^{-1}} = Ye^X Y^{-1}$$

Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

Produit scalaire euclidien et produit scalaire hermitien

Dans $\mathbb{R}^n$, on peut définir le produit scalaire (à valeurs dans $\mathbb{R}$) des vecteurs $x = (x_1, x_2, \cdots, x_n)$ et $y = (y_1, y_2, \cdots, y_n)$ par $x.y = x_1.y_1 + x_2.y_2 + \cdots + x_n.y_n = \sum_{k=1}^{n} x_k.y_k$

Dans $\mathbb{C}^n$, on définira le produit scalaire hermitien (à valeurs dans $\mathbb{C}$) des vecteurs $x = (x_1, x_2, \cdots, x_n)$ et $y = (y_1, y_2, \cdots, y_n)$ par $x.y = \overline{x_1}.y_1 + \overline{x_2}.y_2 + \cdots + \overline{x_n}.y_n = \sum_{k=1}^{n} \overline{x_k}.y_k$

On rappelle que si $x = a + i.b$ alors $\overline{x} = a - i.b$ est son conjugué.

Matrice adjointe

Étant donné une matrice $(a_{ij})_{1\leq i,j\leq n}$, sa matrice *adjointe* est la matrice conjuguée et transposée

$$A^{\dagger} = (a'_{ij})_{1\leq i,j\leq n}, \text{ adjointe de A }, \forall i,j, a'_{ij} = \overline{a_{ji}}$$

Un vecteur dans $\mathbb{C}^n$ peut être vu comme une "matrice colonne" avec n lignes et une seule colonne. Son adjoint est donc une "matrice ligne" avec une seule ligne et n colonnes. Le produit scalaire hermitien entre les deux vecteurs peut s'écrire comme le produit matriciel suivant :

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, x.y = x^{\dagger} \times y$$

Matrices hermitiennes et matrices unitaires

définition : matrice hermitienne Une matrice hermitienne est une matrice auto-adjointe, elle est également à sa matrice adjointe

$$A \text{ est une matrice hermitienne} \iff A = A^*$$

définition : matrice unitaire Une matrice unitaire U est telle que son inverse est sa matrice adjointe.

$$U^\dagger = U^{-1} \text{ soit } U \times U^\dagger = U^\dagger \times U = I$$

Une matrice peut être à la fois hermitienne et unitaire, c'est le cas des portes de la porte H et des portes de Pauli en particulier.

Propriétés des matrices hermitiennes

Une matrice hermitienne

- est diagonalisable et la matrice de passage est une matrice unitaire ;
- a des valeurs propres réelles (à valeurs dans $\mathbb{R}$) ;

Propriétés des matrices unitaires

Une matrice unitaire

- est inversible (et son inverse est sa matrice adjointe) ;
- est diagonalisable et la matrice de passage est une matrice unitaire ;
- possède une matrice adjointe qui est également unitaire (puisque étant son inverse) ;
- possède des colonnes qui forment une base orthonormale de $\mathbb{C}^n$ vis-à-vis du produit scalaire hermitien ;
- est normale (elle commute avec son adjointe, c'est évident puisque ce produit vaut l'identité) ;
- a des valeurs propres qui sont complexes (pas forcément réelles) mais dont la norme est égale à 1, elles sont donc toutes de la forme $e^{i\theta}$;
- peut s'écrire sous la forme d'une exponentielle de matrice e^{iH} où H est une matrice hermitienne (et donc iH est anti-hermitienne).

Une matrice unitaire transforme une base orthonormale en une autre base orthonormale.

Matrices unitaires et produit scalaire

$$Ux.Uy = (Ux)^\dagger \times Uy = x\dagger \times U^\dagger \times U \times y$$

$$\text{mais U est unitaire donc } U^\dagger \times U = \mathbb{I} \text{ et par conséquent}$$

$$Ux.Uy = x^\dagger \times y = x.y$$

On a donc $Uy.Uy = x.y$

Les opérateurs unitaires conservent le produit scalaire, ce qui signifie qu'ils ne changent ni les normes ni les angles entre vecteurs.

Disclaimer : ceci n'est pas un cours de physique quantique ! ! ! !

Plan

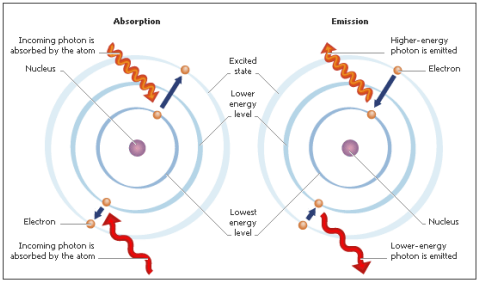
6 La superposition

7 L'intrication

Quantas

Les objets quantiques n'évoluent pas de manière coninue. Ils possèdent différents états *discrets*, correspondant à des états énergétiques identifiés, séparés par des *quanta*.

Dans le cas des différents états d'excitation d'un électron, on aura la chose suivante :



L'électron ne "passe" pas d'une orbite à une autre, il est dans toutes les orbites à la fois, avec différentes probabilités de l'y trouver à cet endroit

Etats superposés

Un objet quantique est **simultanément** dans plusieurs états à la fois, c'est le phénomène de **superposition d'états**.

ATTENTION : ce concept est très contre-intuitif

- Les électrons sont sur plusieurs orbites d'un atome en même temps
- les particules ont des *spin* de valeurs inverses.. en même temps
- les photons peuvent avoir différentes sortes de polarisation ... en même temps
- un même photon peut être simultanément dans deux fibres optiques
- dans une boucle supraconductrice, le courant circulent à la fois dans le sens direct et dans le sens rétrograde

On identifie les états de base par des numéros. Un état $|\Psi\rangle$ sera une composition de ces états de la forme

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

Effondrement quantique

En physique quantique, observer, c'est consommer de l'information. En observant un état superposé, on va effondrer celui-ci sur l'un des états de bases qui le composent. Ensuite, il ne bougera plus et restera à jamais ainsi, comme s'il avait "choisi sont camp".

Si on considère l'état du slide précédent

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

L'observer donnera soit $|1\rangle$, $|2\rangle$, $|3\rangle$ ou $|4\rangle$.

Si on observe, par exemple $|3\rangle$, les mesure suivantes donneront **toujours** $|\Psi\rangle = |3\rangle$

Densités de probabilités

Dans la forrmulation

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

Les termes α à δ sont des nombres à valeurs dans $\mathbb{C}$, ou **densités de probabilités**.
Elles expriment les probabilités que $|\rangle\,\Psi$ est à la fois dans les états $|1\rangle$, à $|4\rangle$. Ce ne sont pas des probabilités "classiques", au sens de Kolmogorov.

Si on mesure $|\Psi\rangle$, il y a une probabilité $|\alpha|^2$ de mesurer $|0\rangle$, $|\beta|^2$ de mesurer $|1\rangle$, $|\gamma|^2$ de mesurer $|2\rangle$ et $|\delta|^2$ de mesurer $|3\rangle$

On a en revanche, il y a 100% de chances de mesure l'un des états, d'où la **condition de normalisation**

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Si on sait reproduire $|\Psi\rangle$ à volonté, on peut, de manière probabiliste, connaître les valeurs des carrés des modules, en faisant suffisament de mesures.

Plan

6 La superposition

7 L'intrication

Le paradoxe EPR

L'intrication est une notion fondamentale en physique quantique. Elle aa été sujette à de nombreuses controverses, dont le célèbre paradoxe EPR, dû à Einstein, Podolsky et Rosen.

Il faudra attendre 1982 et l'expérience de Alain Aspect pour clore le débat. Alain Aspect obtiendra par la suite le Prix Noble de Physique en 2022.

Qu'est-ce que l'intrication ?

Lorsque des objets quantiques interagissent, elles forment un système, ou **état intriqués**.

Les objets intriqués ne peuvent plus être considérés de manière autonome, il faut considérer l'ensemble du système intriqué, en particulier **agir sur une particule** c'est **agir sur l'état intriqué tout entier**.

En particulier, observer l'un quelconque des composants d'un état intriqué provoque son effondrement et l'effondrement de l'ensemble de l'état intriqué.

La programmation quantique, c'est quoi ?

La programmation quantique consiste à :

- utiliser la superposition pour accélérer le calcul sur n qubits
- utiliser l'intrication pour construire des interactions complexes
- **mais** on ne peut mesurer qu'un seul des 2^n état possible

La programmation quantique, c'est construire un opérateur unitaire, sur les qubits, tel que l'état mesuré, ou le plus probablement mesuré, représentera la solution cherchée pour le problème concerné.

La notation de Dirac

En informatique quantique, on utilisera la notation de Dirac. Les vecteurs de $\mathbb{C}^n$ ne seront pas notés x mais $|x\rangle$
Cette notation se nomme "ket", $|x\rangle$ se lira "ket x". Elle correspond à un vecteur écrit "en colonne" soit $\begin{pmatrix} x_1 \\ x_2 \\ . \\ \vdots \\ x_n \end{pmatrix}$.
L'adjoint d'un vecteur $x \in \mathbb{C}^n$ écrit en colonne est écrit "en ligne" , soit $x^\dagger = (\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n})$
Avec la notation de Dirac, l'adjoint de $|x\rangle$ sera noté $\langle x|$, cette forme se nomme "bra" et lire "bra x".

Produit scalaire hermitien et notation de Dirac

Le produit scalaire hermitien peut être écrit comme le produit d'une matrice "ligne" et d'une matrice "colonne" :

$$\begin{aligned} x.y = \overline{x_1}.y_1 + \overline{x_2}.y_2 + \cdots + \overline{x_n}.y_n &= \sum_{k=1}^{n} \overline{x_k}.y_k \\ &= (\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}) \times \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &= \langle x|y\rangle \end{aligned}$$

La norme d'un vecteur est quant à elle donnée par

$$||x|| = \sqrt{\langle x|x\rangle}$$

Matrices et notation de Dirac

Si A est une matrice de $\mathbb{C}^{n\times n}$ représentant une application linéaire, le produit simplement noté $A|x\rangle$.

Si la matrice représente une forme hermitienne, elle est associée à une forme hermitienne F telle que

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x,y) = x^\dagger A y$$

En utilisant la notation de Dirac, l'équation précédente s'écrira

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x,y) = \langle x|A|y\rangle$$

Base canonique et notation de Dirac

L'espace vectoriel $\mathbb{C}^2$ dispose d'une base canonique : $\begin{pmatrix}1\\0\end{pmatrix}$ et $\begin{pmatrix}0\\1\end{pmatrix}$.

Dans la notation de Dirac, on écrira

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Les vecteurs $|0\rangle$ et $|1\rangle$ forment la **base canonique** de $\mathbb{C}^2$.

ATTENTION ! ! ! !, le vecteur $|0\rangle$ n'est pas le vecteur nul : $\overrightarrow{0} = \begin{pmatrix}0\\0\end{pmatrix}$

Produit tensoriel et notation de Dirac

Quand on manipule plusieurs qubits, on va rapidement devoir manipuler des produits tensoriels de ces qubits.

$$\text{On notera } |0\rangle \otimes |0\rangle = |00\rangle \text{ et plus généralement si } (x, y) \in \{0, 1\}^2, |x\rangle \otimes |y\rangle = |xy\rangle$$

Le plus souvent, on n'utilise pas le symbole $\otimes$ qui devient implicite et on pourra écrire

$$|01\rangle\,|0\rangle = |010\rangle$$

Base canonique sur plusieurs qubits

Si l'on dispose de n qubits, on est dans $\mathbb{C}^{2^n}$, qui est isomorphe à $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$
On construit les bases canoniques en construisant les produits tensoriels avec les bases canoniques de $\mathbb{C}^2$. Ainsi $\mathbb{C}^4$ a comme base canonique $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1.\begin{pmatrix}1\\0\end{pmatrix}\\0.\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1.\begin{pmatrix}0\\1\end{pmatrix}\\0.\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

Plan

8 Les circuits quantique

9 Les opérateurs sur 1 seul qubits

10 Les opérateurs sur 2 à n qubits

11 Les circuits sont des matrics

12 Mesures

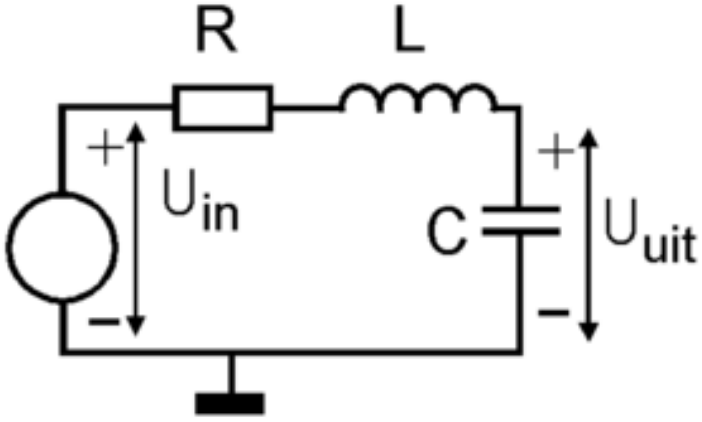
Programmation quantique à portes

Dans la programmation quantique à portes, on programme l'opérateur unitaire sous la forme d'un "circuit"

- le circuit est composé de différentes étapes,
- le circuit est un assemblage de composants génériques, plus simples.

ATTENTION : Un circuit quantique est une manière "graphique" de décrire une matrice $2^n \times 2^n$ potentiellement très complexe.

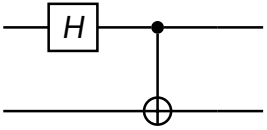
Ceci est un circuit (électrique)



Ceci n'est pas une pipe

Ceci n'est pas un circuit, ceci est une matrice

le circuit suivant construit une *paire EPR*



On verra que ce circuit correspond à la matrice

$$\frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

Les qubits

Un qubit est un vecteur de $\mathbb{C}^2$, contrairement à un bit, il ne prend pas que les valeurs 0 et 1. Un qubit est un état quantique écrit ainsi

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ avec }, \alpha \in \mathbb{C}, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Les valeurs α et β sont des *densités de probabilité*, en mesurant $|\phi\rangle$ on aura

- la valeur $|0\rangle$ avec une probabilité de $|\alpha|^2$
- la valeur $|1\rangle$ avec une probabilité de $|\beta|^2$

Mesure d'un qubit et effondrement

On mesure un qubit $|\phi\rangle$ par rapport à une base orthonormée $(|v_1\rangle, |v_2\rangle)$ ou il s'écrit $|\phi\rangle = \alpha |v_1\rangle + \beta |v_2\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$

La mesure est effectuée grâce à un opérateur dont on peut mesurer les vecteurs propres. Mesurer un état provoque son *effondrement*. Après une mesure, le qubit s'effondre sur l'une de ses deux composantes, et il reste, il devient donc toujours soit $|v_1\rangle$ soit $|v_2\rangle$

Mesurer c'est **perdre de l'information**, mais on est obligé de faire des mesures pour avoir des résultats.

Plan

8 Les circuits quantique

9 Les opérateurs sur 1 seul qubits

10 Les opérateurs sur 2 à n qubits

11 Les circuits sont des matrics

12 Mesures

Zoologie des opérateurs sur 1 qubit

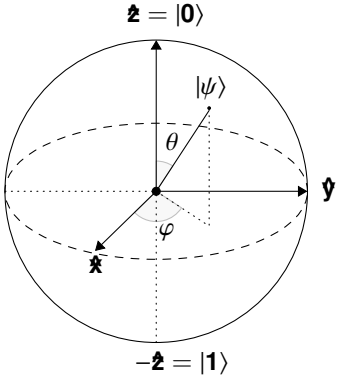
Les opérateurs sur 1 qubit sont des matrices unitaires dans $\mathbb{C}^{2\times 2}$
On va détailler

- la porte de Hadamard
- les portes de Pauli
- les portes de Clifford
- les portes paramétrées

63/370

La sphère de Bloch

La sphère de Bloch est un moyen classique de représenter un qubit. C'est la vue en perspective d'une projection d'un hyperplan à trois dimensions de $\mathbb{C}^2$



Construire la sphère de Bloch 1/2

Un état quantique est un vecteur $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec α et β des nombres complexes tels que $\|\alpha\|^2 + \|\beta\|^2 = 1$. On peut noter α et β sous formes polaires

$$\exists! r_1 \in [0;1], \exists! \psi_1 \in [0;2\pi[, \alpha = r_1.e^{i\phi_1}$$
$$\exists! r_2 \in [0;1], \exists! \psi_2 \in [0;2\pi[, \beta = r_2.e^{i\phi_2}$$

et donc

$$\begin{aligned} |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle &= r_1.e^{i\phi_1}|0\rangle + r_2.e^{i\phi_2}|1\rangle \\ &= e^{i\phi_1}(r_1|0\rangle + r_2 e^{i(\phi_2-\phi_1)}|1\rangle) \\ &= e^{i\phi_1}(r_1|0\rangle + r_2 e^{i\phi}|1\rangle) \text{ avec } \phi = \phi_2 - \phi_1 \end{aligned}$$

On ne peut pas mesurer la phase $e^{i\phi_1}$ dont la norme est 1, donc $|\Psi\rangle \equiv e^{-i\phi_1}|\Psi\rangle$, il est légitime d'ignorer le facteur $e^{i\phi_1}$ dans l'équation précédente et donc

$$|\Psi\rangle \equiv r_1|0\rangle + r_2 e^{i\phi}|1\rangle, r1, r2 \in [0;1], \phi \in [0;2\pi[$$

Construire la sphère de Bloch 2/2

Les carrés des modules composants en $|0\rangle$ et $|1\rangle$ vaut 1, par conséquent ${r_1}^2 + {r_2}^2 = 1$, ce qui est analogue à l'équation $cos^2(\theta) + sin^2(\theta) = 1$

Il est donc possible de trouver un angle θ tel que $r_1 = cos(\frac{\theta}{2})$ et $r_2 = sin(\frac{\theta}{2})$,

comme r_1 et r_2 sont dans $[0; 1]$ alors $\frac{\theta}{2}$ varie dans $[0, \pi]$. On peut donc écrire $|\Psi\rangle$ sous la forme $|\Psi\rangle = cos(\frac{\theta}{2})\,|0\rangle + sin(\frac{\theta}{2})e^{i\phi}\,|1\rangle$,

un état quantique est donc totalement défini par deux angles $\theta \in [0, \pi]$ et $\phi \in [0; 2\pi]$

Note : Une construction plus algébrique de la sphère de Bloch est possible, en exploitant le corps des quaternions.

La porte X, ou porte NOT

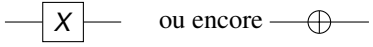
La porte X a les effets suivants sur la base canonique (bit flip)

- le qubit $|0\rangle$ devient $|1\rangle$, soit $X|0\rangle = |1\rangle$
- le qubit $|1\rangle$ devient $|0\rangle$, soit $X|1\rangle = |0\rangle$

La porte X est représentée par la matrice unitaire suivante

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

La porte X est représentée ainsi



La porte X réalise une **rotation** d'un angle π autour de l'axe X de la sphère de Bloch.

La porte Z

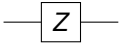
La porte Z a les effets suivants sur la base canonique (phase flip)

- le qubit $|0\rangle$ devient $0\rangle$, qui est invariant, soit $Z|0\rangle = |0\rangle$
- le qubit $|1\rangle$ devient $-|1\rangle$, soit $Z|1\rangle = -|1\rangle$

La porte Z est aussi appelée "porte d'inversion de phase" ou *phase flip*.
Elle est représentée par la matrice unitaire suivante

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

La porte Z est représentée ainsi



La porte Z réalise une **rotation** d'un angle π autour de l'axe Z de la sphère de Bloch.

La porte Y

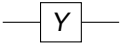
La porte Y a les effets suivants sur la base canonique

- le qubit $|0\rangle$ devient $i|1\rangle$, soit $Y|0\rangle = i|1\rangle$
- le qubit $|1\rangle$ devient $-i|0\rangle$, soit $Y|1\rangle = -i|0\rangle$

La porte Y réalise une **rotation** d'un angle π autour de l'axe Y de la sphère de Bloch.
Elle est représentée par la matrice unitaire suivante

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

La porte Y est représentée ainsi



$Y = iXZ$: Y est un bit filp (X), plus un phase flip (Z), plus une modification de phase.

Superposition

La base canonique n'est pas la seule base orthonormée de $\mathbb{C}^2$. Il est classique d'utiliser la base $|+\rangle, |-\rangle$ définie par

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

Ces deux états sont très importants car ils sont uniformément superposés, quand on mesure $|+\rangle$ ou $|-\rangle$ on a toujours

- $(\frac{1}{\sqrt{2}})^2 = 50\%$ de chance de mesurer $|0\rangle$
- 50% de chance de mesurer $|1\rangle$

On observera aussi que $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ et $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

La porte H, ou porte de Hadamard

La porte de Hadamard est de loin la plus célèbre de toutes les portes quantiques et de loin l'une des plus utilisées. Elle doit son nom au mathématicien français Jacques Hadamard.

La porte H transforme la base $(|0\rangle, |1\rangle)$ en la base $(|+\rangle, |-\rangle)$ et inversement. Elle introduit la superposition d'états

- $H|0\rangle = |+\rangle$ et $H|1\rangle = |-\rangle$
- $H|+\rangle = |0\rangle$ et $H|-\rangle = |1\rangle$

La porte H est représentée par la matrice unitaire suivante

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

On remarquera que

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}) = \frac{1}{\sqrt{2}} (X + Z)$$

Racines carrées de portes

Toutes les portes à 1 qubits sont des rotations dans $\mathbb{C}^2$, elles ont des racines carrées.

La matrice $\sqrt{X} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$ est telle que son carré est la matrice X

Il est possible de trouver des racines n-ièmes de toutes les portes.

On verra comment ces portes sont utiles pour construire une boite à outils universelle permettant de construire toutes les portes à n qubits.

Plan

8 Les circuits quantique

9 Les opérateurs sur 1 seul qubits

10 Les opérateurs sur 2 à n qubits

11 Les circuits sont des matrics

12 Mesures

Représenter les états intriqués algébriquement

Certains états à n qubits peuvent se factoriser, par exemple

$$\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle \otimes |-\rangle$$

En revanche, certains ne peuvent pas se factoriser, comme celui-ci (appelé **paire EPR**)

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Les états non factorisables ne permettent pas de manipuler les qubits un par un, il faut considérer les n qubits ensemble, ils correspondent aux **états intriqués**

L'espace vectoriel des états factorisables a pour dimension $2n$, à comparer à la dimension 2^n de l'espace des qubits

Il y a **beaucoup plus** d'états intriqués que d'états non-intriqués.

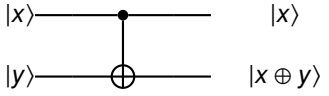
L'intrication et la porte CNOT

La porte CNOT, ou porte CX, est une porte NOT (ou porte X) qui agit sur le second qubit mais qui est contrôlée par le premier qubit.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ donc } CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

L'effet d'une porte CNOT sur 2 qubit représenté par $|xy\rangle$ (x et 0 sont des bits) :

- si x = 0, ne pas toucher à $|y\rangle$, on obtient $|0y\rangle$ inchangé à la fin
- si x = 1, inverser y, on obtient donc $|1\neg y\rangle$



D'une manière synthétique, la porte CNOT ne touche pas le premier qubit $|x\rangle$ mais transforme le second qubit $|y\rangle$ en $|x \oplus y\rangle$.

Portes contrôlées (1/3)

La porte CNOT est la principale porte contrôlée. Les portes contrôlées

- permettent un traitement du type *if-then-else*
- s'appuient sur le phénomène d'intrication quantique

Si U est un opérateur unitaire de $\mathbb{C}^2$, il est algébriquement simple de définir une porte contrôlée CU qui est un opérateur unitaire de $\mathbb{C}^4$.
Considérons les *projecteurs* sur $|0\rangle$ et $|1\rangle$ (qui ne sont pas des opérateurs unitaires)

$$|0\rangle \times \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } |1\rangle \times \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Alors la porte CU définie par

$$CU = (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U$$

est une porte contrôlée unitaire : elle applique U sur le second qubit si le premier vaut $|1\rangle$

Portes contrôlées (2/3)

Il est simple de voir que CU est unitaire

$$CU = (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

et

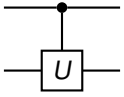
$$\begin{aligned} CU \times (CU)^\dagger &= (|0\rangle\langle 0| \otimes I + (|1\rangle\langle 1|) \otimes U) \times (|0\rangle\langle 0| \otimes I + (|1\rangle\langle 1|) \otimes U)^\dagger \\ &= (|0\rangle\langle 0|0\rangle\langle 0|) \otimes (I \times I) + (|1\rangle\langle 1|1\rangle\langle 1|) \otimes (U \times U^\dagger) + \\ &(|0\rangle\langle 0|1\rangle\langle 0|) \otimes (I \times U^\dagger) + (|1\rangle\langle 1|0\rangle\langle 0|) \otimes (U \times I) \\ &= (|0\rangle\langle 0|0\rangle\langle 0|) \otimes (I \times I) + (|1\rangle\langle 1|1\rangle\langle 1|) \otimes (U \times U^\dagger) \\ &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes I = I \otimes I = I \end{aligned}$$

Portes contrôlées (3/3)

$$\begin{aligned} CU|0x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|0\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|0\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|0\rangle \otimes U|x\rangle) \\ &= |0\rangle \otimes I|x\rangle = |0\rangle \otimes |x\rangle = |0x\rangle \end{aligned}$$

$$\begin{aligned} CU|1x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|1\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|1\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|1\rangle \otimes U|x\rangle) \\ &= |1\rangle \otimes U|x\rangle = |1\rangle \otimes U|x\rangle \end{aligned}$$

Un porte U contrôlée sera dessinée comme ceci dans les circuits quantiques :



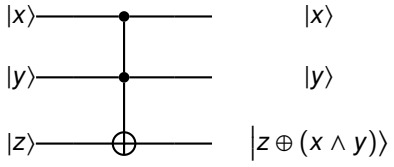
Il est légitime de faire des portes doublement contrôlées

Porte de Toffoli

La porte de Toffoli est une porte opérant sur 3 qubits, c'est une porte CCNOT (NOT à double contrôle)

$$CCX = \begin{pmatrix} I & 0 \\ 0 & CX \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Son effet est le suivant :



Porte SWAP 1/2

La porte SWAP permet d'échanger deux qubits. Les actions sur la base canonique de $\mathbb{C}^4$ sont les suivants :

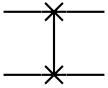
- $SWAP\,|00\rangle = |00\rangle$ (intervertir deux 0 donne toujours deux 0 à la fin) ;
- $SWAP\,|01\rangle = |10\rangle$;
- $SWAP\,|10\rangle = |01\rangle$;
- $SWAP\,|11\rangle = |11\rangle$ (intervertir deux 1 donne toujours deux 1 à la fin).

À partir de ces images des vecteurs de base, on peut déduire la matrice suivante :

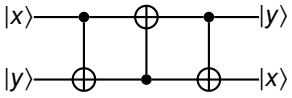
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Porte SWAP 2/2

La porte SWAP s'écrit ainsi dans les circuits :



Elle peut s'implémenter à l'aide de trois portes CNOT



Porte de Fredkin 1/2

La porte de Fredkin est une porte SWAP contrôlée : elle échange les deux derniers qubits si le premier vaut $|1\rangle$.

Son effet sur les vecteur de base de $\mathbb{C}^8$ sera donc le suivant :

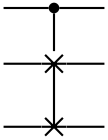
- $F|000\rangle = |000\rangle$
- $F|001\rangle = |001\rangle$
- $F|010\rangle = |010\rangle$
- $F|011\rangle = |011\rangle$
- $F|100\rangle = |100\rangle$
- $F|101\rangle = |110\rangle$
- $F|110\rangle = |101\rangle$
- $F|111\rangle = |111\rangle$

Porte de Fredkin 2/2

La matrice de la porte de Fredkin se déduit des actions sur les vecteurs de base :

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

Elle est représentée ainsi



Racine carrée de la porte SWAP 1/2

La porte SWAP est une matrice unitaire, c'est une rotation dans $\mathbb{C}^4$, on peut lui trouver une racine carrée.
Si $\overline{CX}$ représente une porte CX "tête bêche", alors on peut écrire

$$SWAP = CX \times \overline{CX}\ timesCX$$

On en déduit que $\sqrt{SWAP} = CX \times \sqrt{\overline{CX}} \times CX$, en effet, il est simple de vérifier que

$$\begin{aligned}\sqrt{SWAP} \times \sqrt{SWAP} &= (CX \times \sqrt{\overline{CX}} \times CX) \times (CX \times \sqrt{\overline{CX}} \times CX) \\ &= CX \times \sqrt{\overline{CX}} \times \sqrt{\overline{CX}} \times CX \\ &= CX \times \overline{CX} \times CX \\ &= SWAP\end{aligned}$$

Racine carrée de la porte SWAP 2/2

De la même manière qu'on a établi la matrice de $\overline{CX}$ il est simple d'établir la matrice de $\sqrt{\overline{CX}}$:

$$\sqrt{\overline{CX}} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix}$$

Par conséquent, la matrice de $\sqrt{SWAP}$ va s'écrire de la manière suivante :

$$\begin{aligned} \sqrt{SWAP} &= CX \times \sqrt{\overline{CX}} \times CX \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 1-i & 0 \\ 0 & 1-i & 1+i & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \end{aligned}$$

Plan

8 Les circuits quantique

9 Les opérateurs sur 1 seul qubits

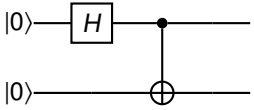
10 Les opérateurs sur 2 à n qubits

11 Les circuits sont des matrics

12 Mesures

Base de Bell et circuit EPR

Le circuit suivant (que nous avons déjà rencontré) implémente une "paire EPR"



Il met en oeuvre à la fois de la superposition (via la porte H) et de l'intrication (via la porte CNOT).
Il change la base canonique de $\mathbb{C}^2$ en la **base de Bell**, orthonormale, formée d'états intriqués.

- l'état $|00\rangle$ est envoyé sur la paire EPR, $|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- l'état $|01\rangle$ est envoyé sur $|\Psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- l'état $|10\rangle$ est envoyé sur $|\Phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- l'état $|11\rangle$ est envoyé sur $|\Psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Fonctionnement du circuit EPR

On peut analyser le fonctionnement de ce circuit de la façon suivante : L'état de départ est $|0\rangle \otimes |0\rangle = |00\rangle$

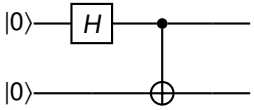
On applique une porte H au premier qubit, état devient

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

On applique ensuite une porte CNOT qui laisse $|00\rangle$ inchangé, mais qui transforme $|10\rangle$ en $|11\rangle$. Il en résulte la paire EPR.

$$\text{Paire EPR} : \mathit{CNOT}(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Calcul de la matrice de la paire EPR 1/3



Le circuit EPR se compose de deux étapes :

- une paire H sur le premier qubit, rien sur le second qbit ;
- une porte CNOT sur les deux qubits ;

La première étape peut s'écrire comme le produit tensoriel de la porte H et de l'identité :

$$Step1 = H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Calcul de la matrice de la paire EPR 2/3

On rappelle que la porte CNOT s'écrit ainsi

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

Dans l'exécution du circuit, on applique d'abord $H \otimes I$ puis CNOT, on applique donc le produit matriciel $CNOT \times (H \otimes I)$.

Attention : les matrices se composent comme les applications, le produit est en ordre inverse de l'application des matrices.

Calcul de la matrice de la paire EPR 3/3

Le calcul matriciel donne le résultat suivant

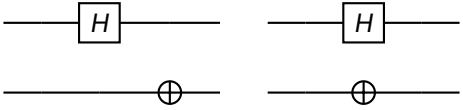
$$CNOT \times (H \otimes I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

On rappelle que les colonnes de cette matrice sont les images des vecteurs de la base canonique. Dans le cas du circuit de la paire EPR, on retrouve sans surprise les états de Bell.

Attention aux étapes !

Les étapes, ou "colonnes", des circuits quantiques sont très importants. Les deux circuits suivants sont très différents



Le premier correspond à $(I \otimes X) \times (H \otimes I)$, le second correspond à $H \otimes X$

Plan

8 Les circuits quantique

9 Les opérateurs sur 1 seul qubits

10 Les opérateurs sur 2 à n qubits

11 Les circuits sont des matrics

12 Mesures

Observables

Les observables correspondent à des grandeurs physiquesqui peuvent être observées et donc mesurées. On doit ce terme à Werner Heisenberg.
Mathématiquement, Les observables sont des opérateurs dans des espaces de Hilbert tels que

- l'opérateur observable A est linéaire, il sera représenté par une matrice ;
- les mesures correspondent aux valeurs propres de l'observable, celles-ci doivent être réelles, ce qui impose que l'observable A soit hermitien donc auto-adjoint ;
- les vecteurs propres de l'observable sont orthogonaux, et ils forment une base de l'espace de Hilbert ;
- cette base est normalisable, on peut modifier A pour disposer d'un observable dont les vecteurs propres forment une base orthonormée.

Fondamentalement, quand on mesure une grandeur physique par le biais d'un observable, on mesure l'une des valeurs propres de l'observable, ou plutôt la probabilité de l'occurrence d'une valeur propre d'observable.

Mesures selon Z

On ne mesure pas un qubit par rapport à une base (par exemple $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$, on observe selon un opérateur hermitien dont les vecteurs propres forment la base en question.

Considérons à présent l'opérateur Z de Pauli dont la matrice est

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

Il est trivial de constater que cet opérateur dispose de deux valeurs propres, 1 et -1, et que

$$Z|0\rangle = |0\rangle \text{ et } Z|1\rangle = -|1\rangle$$

La base canonique est en fait la base de vecteurs propres de Z. Réaliser une mesure dans cette base (canonique) revient à réaliser une observation, donc une mesure de valeur propre, par le biais de 2 pris comme un observable.

Mesure selon X

Intéressons-nous à présent à la base, dite de Hadamard, de $\mathbb{C}^2$, à savoir $(|+\rangle, |-\rangle)$.

Cette fois-ci, c'est à l'opérateur X qu'on va s'intéresser. On rappelle que

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

Il est simple de vérifier que ($|+\rangle$ et $|-\rangle$) sont les vecteurs propres de X, et qu'ils font associés aux valeurs propres 1 et -1. En effet

$$X|+\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) == \frac{1}{\sqrt{2}}(ket1 + |0\rangle) = |+\rangle$$
$$X|-\rangle = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) == \frac{1}{\sqrt{2}}(ket1 - |0\rangle) = -|1\rangle$$

Mesurer un qubit dans la base de Hadamard revient à effectuer une mesure grâce à X utilisé comme un observable.

Autres opérateurs de mesures

On pourrait mesurer selon l'opérateur Y. Ses valeurs propres sont 1 et -1 et ses les vecteurs propres, qui figurent sur la sphère de Bloch, sont $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Il est à noter que l'opérateur H, qui est égal à $\frac{1}{\sqrt{2}}(X + Z)$, est également un observable, même s'il est rarement utilisé en tant que tel dans l'informatique quantique.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

L'algorithme de Deutsch-Josza à 2 qubits

Cette section décrit un algorithme très simple et son implémentation sous la forme d'un circuit quantique. Il n'est pas très élaboré, mais va permettre de prendre en main différentes notions propres à l'informatique quantique.

Cet algorithme a été défini en 1992 par David Deutsch et Rochard Josza . Il a été amélioré en 1998 par Richard Cleve, Artur Ekert, Chiara Macchiavello, et Michele Mosca.

L'algorithme de Deutsch-Josza se formule ainsi : étant donné une fonction booléenne $f : \{0, 1\} \rightarrow \{0, 1\}$, comment déterminer si f est constante ?

Approche classique

Une analyse rapide du problème montre qu'il y a 4 cas possible pour une telle fonction booléenne :

1. $f(0) = 0, f(1) = 1, f(0) \oplus f(1) = 1$
2. $f(0) = 1, f(1) = 0, f(0) \oplus f(1) = 1$
3. $f(0) = 0, f(1) = 0, f(0) \oplus f(1) = 0$
4. $f(0) = 1, f(1) = 1, f(0) \oplus f(1) = 0$

Soit deux cas avec des fonctions constantes et deux cas avec des fonctions uniformes.
On peut déterminer le type de la fonction en testant la valeur de $f(0) \oplus f(1)$ avec l'opérateur XOR, noté $\oplus$.

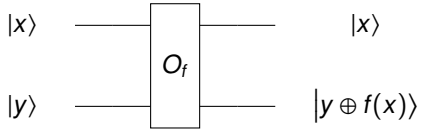
Si f est constante, on aura $f(0) \oplus f(1) = 0$, mais si elle est uniforme, on aura $f(0) \oplus f(1) = 1$.

Avec un ordinateur classique, il faudra deux appels à la fonction f pour déterminer le type de la fonction.

Approche quantique : Oracle

La première étape consiste en la construction d'un *oracle*. Un oracle O_f est une "boîte noire" dans le circuit qui implémentera la fonction f.

Cet opérateur doit être linéaire et inversible.



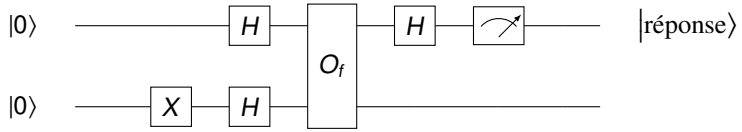
L'oracle agit ainsi :

- il agit sur 2 qubits, le premier porte l'argument, le second portera le résultat ;
- le premier qubit, l'argument, n'est pas modifié par l'oracle ;
- le second qubit est XORé avec la valeur $f(x)$

Cet oracle est inversible, si on l'applique deux fois, le premier qubit ne changera toujours pas et le second deviendra $|y \oplus x \oplus x\rangle = |y \oplus 0\rangle = |y\rangle$

Circuit quantique implémentant l'algorithme de Deutsch-Josza

L'algorithme de Deutsch-Josza sera implémenté par le circuit suivant :



On peut dès lors commencer à dérouler le fonctionnement de ce circuit. La porte X va passer le second qubit dans l'état $|1\rangle$, on a donc 2 qubits dans l'état $|01\rangle$ avant les portes H. Quand elle s'applique, on va avoir :

$$\begin{aligned}(H\otimes H)\,|01\rangle &= H|0\rangle\otimes H|1\rangle = |+\rangle\otimes|-\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\ &= \frac{1}{2}(|00\rangle+|10\rangle-|01\rangle-|11\rangle) \\ &= \frac{|0\rangle\,(|0\rangle-|1\rangle)}{2}+\frac{|1\rangle\,(|0\rangle-|1\rangle)}{2}\end{aligned}$$

Application de l'Oracle

On applique l'oracle O_f qui est linéaire, son action change l'état précédent en

$$|\phi_1\rangle = \frac{|0\rangle\left(\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle\right)}{2} + \frac{|1\rangle\left(\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle\right)}{2}$$

On distingue ensuite les cas selon les valeurs de $f(0)$ et $f(1)$).

- **Si** $f(0) = 0$, on a $\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle = \left|0 \oplus 0\right\rangle - |1 \oplus 0\rangle = \left|0\right\rangle - |1\rangle$
- **Si** $f(0) = 1$, on a $\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle = \left|0 \oplus 1\right\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle = -(\left|0\right\rangle - |1\rangle)$

De même

- **Si** $f(1) = 0$, on a $\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle = |0 \oplus 0\rangle - |1 \oplus 0\rangle = |0\rangle - |1\rangle$
- **Si** $f(1) = 1$, on a $\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle = |0 \oplus 1\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle = -(\left|0\right\rangle - |1\rangle$

103/370

Une astuce de calcul

On va alors recourir à une astuce de notation qui est très courante en arithmétique booléenne en introduisant des puissances de -1, les lignes précédentes peuvent se réécrire ainsi :

$$\big|0 \oplus f(0)\big\rangle - \big|1 \oplus f(0)\big\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$$
$$\big|0 \oplus f(1)\big\rangle - \big|1 \oplus f(1)\big\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle)$$

Si l'on reporte cela dans l'état précédent $|\phi_1\rangle$, on peut écrire

$$\begin{aligned}|\phi_1\rangle &= \frac{|0\rangle\left(\big|0 \oplus f(0)\big\rangle - \big|1 \oplus f(0)\big\rangle\right)}{2} + \frac{|1\rangle\left(\big|0 \oplus f(1)\big\rangle - \big|1 \oplus f(1)\big\rangle\right)}{2} \\ &= \frac{(-1)^{f(0)}\,|0\rangle\,(|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(1)}\,|1\rangle\,(|0\rangle - |1\rangle)}{2}\end{aligned}$$

Suite du calcul

On a vu que multiplier par un nombre dont la norme est 1 ne change rien au fonctionnement et en particulier ne change rien à la mesure. L'état $|\phi_1\rangle$ est donc équivalent à l'état $|\phi_2\rangle = (-1)^{f(0)}|\phi_1\rangle$ et on notera alors que

$$\begin{aligned}
|\phi_2\rangle &= \frac{(-1)^{f(0)}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(0)}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)}{2} \\
&= \frac{|0\rangle(|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(0)+f(1)}|1\rangle(|0\rangle - |1\rangle)}{2} \\
&= \frac{|0\rangle + (-1)^{f(0)+f(1)}|1\rangle}{\sqrt{2}} \otimes |-\rangle
\end{aligned}$$

Fin du calcul

Distinguons à présent selon les valeurs relatives de $f(0)$ et $f(1)$ On notera que

- Si $f(0) = f(1)$ alors $f(0) + f(1)$ vaur soit 0 soit 2, donc $(-1)^{f(0)+f(1)}$ vaut 1
- Si $f(0) \neq f(1)$ alors on a une valeur 0 et une valeur 1 dont la sommee fait 1 donc $(-1)^{f(0)+f(1)}$ vaut -1

Par conséquent

- Si $f(0) = f(1)$ alors $|\phi_2\rangle = \frac{|0\rangle(|0\rangle-|1\rangle)}{2} + \frac{|1\rangle(|0\rangle-|1\rangle)}{2} = \frac{(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2}$
- Si $f(0) \neq f(1)$ alors $|\phi_2\rangle = \frac{|0\rangle(|0\rangle-|1\rangle)}{2} - \frac{|1\rangle(|0\rangle-|1\rangle)}{2} = \frac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2}$

On peut condenser cette équation en introduisant les notations $|+\rangle$ et $|-\rangle$

- Si $f(0) = f(1)$ alors $|\phi_2\rangle = \frac{(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2} = |+\rangle|-\rangle$
- Si $f(0) \neq f(1)$ alors $|\phi_2\rangle = \frac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2} = |-\rangle|-\rangle$

Analyse

En ne s'intéressant qu'au premier qubit

- Si $f(0) = f(1)$ alors le premier qubit vaudra $|+\rangle$
- Si $f(0) \neq f(1)$ alors le premier qubit vaudra $|-\rangle$

En appliquant la dernière porte H sur le dernier qubit

- Si $f(0) = f(1)$ alors le premier qubit vaudra $H|+\rangle = |0\rangle$
- Si $f(0) \neq f(1)$ alors le premier qubit vaudra $H|-\rangle = |1\rangle$

Il suffira dès lors de mesurer ce qubit pour savoir si f est constante ou non.

Il suffit d'invoquer l'oracle O_f une seule fois pour avoir le résultat, alors que l'approche classique suppose d'évaluer la fonction f deux fois.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini

14 Premiers algorithmes quantique : Bernstein-Vazirini

15 Théorème de non-clonage

16 Boite à outils universelle pour construire les portes

17 Téléportation quantique et codage super-dense

18 Les mathématiques derrière RSA

19 Transformée de Fourier discrète et transformée de Fourier quantique

20 Algorithme de Simon

21 Algorithme de Shor

22 Algorithme de Grover

Enoncé de l'algorithme de Bernstein-Vazirini

L'algorithme de Bernstein-Vazirini peut être vu comme une variation de l'algorithme de Deutsch-Josza. Il a été proposé par Ethan Bernstein et Umesh Vazirani en 1992.

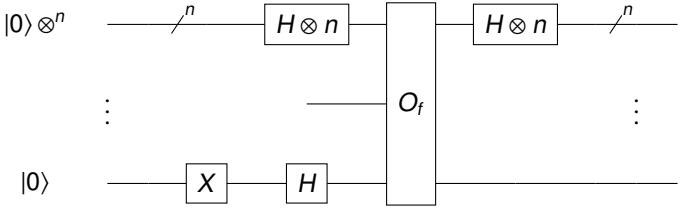
Ici, il s'agit de déterminer de manière efficace un secret codé sur n bits.

Étant donné une chaine s de n bits, on peut construire une fonction f basé sur le produit pointé :

$$f : \{0,1\}^n \to \{0,1\}$$
$$x \mapsto s \cdot x = s_1x_1 \oplus s_2x_2 \oplus \cdots \oplus s_nx_n = s_1x_1 + \cdots + s_nx_n \text{ modulo } 2$$

Connaissant f, et donc l'oracle O_f correspondant, on souhaite trouver la valeur de s.

Circuit associé



110/370

Superposition uniforme - barrière de portes H

L'application de n portes H sur n qubits permet de créer une superposition uniforme de la forme

$$|\phi_0\rangle = \underbrace{|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle}_{ntermers} \otimes |-\rangle$$
$$= \frac{1}{\sqrt{2^{n+1}}}(\underbrace{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}_{\text{n termes}} \otimes (|0\rangle - |1\rangle)$$

que l'on peut écrire ainsi, si x prend toutes les valeurs binaires de 0 à 2^n

$$|\phi_0\rangle = \frac{1}{\sqrt{2^{n+1}}}(\sum_{x=0}^{2^n-1} |x\rangle)(|0\rangle - |1\rangle)$$

Dans cette notation, on écrira

$$|5\rangle = |0101\rangle, |3\rangle = |0011\rangle$$

Application de l'oracle

L'application de l'oracle donne l'état $|\phi_1\rangle$ décrit par

$$|\phi_1\rangle = \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{x=0}^{2^n-1}|x\rangle\right)\left(\left|f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle\right)$$

On sait que f prend les valeurs 0 ou 1, en appliquant le même raisonnement qu'au paragraphe précédent, on en déduit que $|\phi_1\rangle$ est équivalent au qubit $|\phi_2\rangle$

$$|\phi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2^n}}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right) \otimes |-\rangle$$

On peut ignorer le qubit ancillaire dans la suite du calcul, on sait qu'il portera l'état $|-\rangle$
On ne s'intéresse qu'aux n premiers qubits qui seront mesurés à la sortie du circuit.

Application de la seconde barrière de portes H

La superposition uniforme est donnée par

$$|\phi\rangle = \frac{1}{\sqrt{2^{n+1}}}\left(\sum_{x=0}^{2^n-1}|x\rangle\right)$$

Si on applique une porte H sur chaque porte, on aura

$$H|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}H|x\rangle$$

Comment exprimer simplement $H|x\rangle$ avec $x \in \{00..0, \cdots, 11..1\}$?

En utilisant le produit pointé entre deux nombres binaires, on peut écrire

$$H|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}}(-1)^{x\cdot y}|y\rangle$$

113/370

Utilisation du produit pointé

Attention, dans ce qui suit on a 2 qubits, donc $|3\rangle \mapsto |11\rangle$ et surtout $|1\rangle \mapsto |01\rangle$

$$\begin{aligned}
(H \otimes H)|01\rangle &= H|0\rangle \otimes H|1\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) \\
&= \frac{1}{2}((-1)^{00.01}|00\rangle + (-1)^{10.01}|10\rangle + (-1)^{01.01}|01\rangle + (-1)^{11.01}|11\rangle) \\
&= \frac{1}{2}\sum_{x=0}^{3}(-1)^{x.01}|x\rangle
\end{aligned}$$

L'équation $H|y\rangle = \frac{1}{2}\sum_{x=0}^{3}(-1)^{x.y}|x\rangle$ se démontre facilement par récurrence.

Retour à Bernstein-Vazirini

Avant la dernière bordée de porte H on a l'état

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\otimes|-\rangle = |\psi\rangle|-\rangle$$

Appliquons H sur le premier terme $|\psi\rangle$

$$\begin{aligned} H|\psi\rangle &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}H|x\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}}(-1)^{x\cdot y}|y\rangle \\ &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^{n-1}}(-1)^{x\cdot y}|y\rangle \end{aligned}$$

Suite du calcul

$$
\begin{aligned}
H|\psi\rangle &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^{n-1}}(-1)^{x\cdot y}|y\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^{n-1}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}|y\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^{n-1}}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|y\rangle \\
&= \frac{1}{2^n}\sum_{y=0}^{2^{n-1}}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}\right]|y\rangle
\end{aligned}
$$

Discussion et conclusion

La somme précédente peut s'écrire

$$\frac{1}{2^n}\sum_{y=0}^{2^{n-1}}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}\right]|y\rangle = \sum_{y=0}^{2^{n-1}}\alpha_y\,|y\rangle \text{ avec } \alpha_y = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot y}$$

L'indice y va prendre toutes les valeurs entières possibles, il prend en particulier la valeur s, à savoir le secret que l'on cherche, or

$$\alpha_s = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(s)+s\cdot s}$$

Or $f(x) = x.s$ donc

$$\alpha_s = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{s\cdot s+s\cdot s} = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{2(s\cdot s)} = \frac{1}{2^n}\sum_{x=0}^{2^n-1}1 = \frac{2^n}{2^n} = 1$$

Résultat en un seul tir !

L'état final est un état quantique viable sur n qubit donc $\sum_{y=0}^{2^{n-1}} |\alpha_y|^2 = 1$

Mais on sait que $\alpha_s = 1$, par conséquent, tous les autres coefficients α_y sont nuls, donc l'état final

$$\sum_{y=0}^{2^{n-1}} \alpha_y |y\rangle = \alpha_s |s\rangle + \sum_{y \neq s} \alpha_y |y\rangle = |s\rangle + \sum_{y \neq s} 0 |y\rangle = |s\rangle$$

A la fin de l'exécution d'un seul tir, la valeur mesurée sera uniquement $|s\rangle$.

On a le résultat recherché en une seule et unique exécution de l'algorithme.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini

14 Premiers algorithmes quantique : Bernstein-Vazirini

15 Théorème de non-clonage

16 Boite à outils universelle pour construire les portes

17 Téléportation quantique et codage super-dense

18 Les mathématiques derrière RSA

19 Transformée de Fourier discrète et transformée de Fourier quantique

20 Algorithme de Simon

21 Algorithme de Shor

22 Algorithme de Grover

Le théorème de non-clonage des états

Il est légitime de se demander s'il est possible de dupliquer un état quantique, en d'autres termes existe-t-il un opérateur unitaire U tel que $U(|x\rangle|0\rangle) = |x\rangle|x\rangle$.

On peut être tenté de se dire que la porte CNOT permet de faire une telle opération. En effet, si l'on considère les seuls états de base $|0\rangle$ et $|1\rangle$, l'effet de la porte CNOT est $|x\rangle|y\rangle \rightarrow |x\rangle|x \oplus y\rangle$, et donc $|x\rangle|0\rangle \rightarrow |x\rangle|x\rangle$.
Cette relation devient fausse dès lors que $|x\rangle = \alpha|0\rangle + \beta|1\rangle$

Le théorème de non-clonage des états stipule qu'il n'existe pas d'opérateur unitaire U tel que $U(|x\rangle|0\rangle) = |x\rangle|x\rangle$

Démonstration sur 2 qubits

Supposons qu'il existe un opérateur U unitaire tel que $U|x\rangle|0\rangle = |x\rangle|x\rangle$. Par conséquent,

$$U(|00\rangle) = |00\rangle \text{ et } U(|10\rangle) = |11\rangle$$

Par conséquent

$$U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = U(\frac{|00\rangle}{\sqrt{2}}) + U(\frac{|10\rangle}{\sqrt{2}}) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Cependant, on remarque que $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = (\frac{|0\rangle+|1\rangle}{\sqrt{2}})|0\rangle$

On devrait donc avoir

$$\begin{aligned} U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) &= U((\frac{|0\rangle + |1\rangle}{\sqrt{2}})|0\rangle) \\ &= (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \end{aligned}$$

Conclusion

$$U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ et } U(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = (\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + |1\rangle}{\sqrt{2}})$$

On a donc un état dont l'image par U est à la fois un état intriqué $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et un état non intriqué (car factorisé) $(\frac{|0\rangle+|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle+|1\rangle}{\sqrt{2}})$ ce qui est une évidente contradiction.

Par conséquent l'opérateur *U* n'existe pas, ce qui démontre le théorème.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini

14 Premiers algorithmes quantique : Bernstein-Vazirini

15 Théorème de non-clonage

16 Boite à outils universelle pour construire les portes

17 Téléportation quantique et codage super-dense

18 Les mathématiques derrière RSA

19 Transformée de Fourier discrète et transformée de Fourier quantique

20 Algorithme de Simon

21 Algorithme de Shor

22 Algorithme de Grover

Dans cette section

Cette section va aborder les points suivants

- zoologie étendue des portes
- comment construire toutes les portes possibles à 1 qubit (à une approximation près)
- comment construire toutes les portes à 2 qubits puis à n qubits

Rappels :

- les portes et les circuits sont **toujours** des matrices unitaires
- on est dans un espace de Hilbert, on a le droit de parler de convergence de suites

Portes paramétrées

Les portes X, Y et Z sont des rotations d'angle π, les portes paramétrées agissent sur les mêmes axes de la sphère de Bloch, mais avec des angles variables.

Les portes paramétrées sont équivalentes, dans $\mathbb{C}^4$, aux rotations de $\mathbb{C}$, notée $e^{i\theta}$

$$R_X(\alpha) = e^{-i\frac{\alpha}{2}X}, R_Y(\beta) = e^{-i\frac{\beta}{2}Y}, R_z(\gamma) = e^{-i\frac{\gamma}{2}Z}$$

Attention au coefficient $1/2$ **!**.
On rappellera que les matrices X, Y et Z s'écrivent ainsi :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Formes exponentielles des portes paramétrées

Les opérations X, Y et Z sont leurs propres inverses, donc leurs carrés valent l'identité. Par conséquent, si A représente l'un quelconque de ces trois opérateurs, on aura

$$
\begin{aligned}
e^{-i\theta A} = \sum_{n=0}^{+\infty} \frac{(i\theta A)^n}{n!} &= \sum_{p=0}^{+\infty} \frac{(i\theta A)^{2p}}{2p!} - \sum_{p=0}^{+\infty} \frac{(i\theta A)^{2p+1}}{2p+1!} \\
&= \sum_{p=0}^{+\infty} \frac{(-1)^p.\theta^{2n} A^{2p}}{2p!} - i.\sum_{p=0}^{+\infty} \frac{(-1)^p \theta^{2p+1} A.A^{2p}}{2p+1!} \\
&= \sum_{p=0}^{+\infty} \frac{(-1)^p.\theta^{2n}}{2p!} I - i.\sum_{p=0}^{+\infty} \frac{(-1)^p \theta^{2p+1}}{2p+1!} A \\
&= cos((\theta) I - i.sin(\theta) A
\end{aligned}
$$

Forme matricielle des portes paramétrées

Rotation $R_X(\theta)$ par rapport à l'axe X de la sphère de Bloch

$$R_X(\theta) = e^{-i\theta/2X} = cos(\theta/2).\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} - i.sin(\theta/2)\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} = \begin{pmatrix}cos(\theta/2) & -isin(\theta/2)\\isin(\theta/2) & cos(\theta/2)\end{pmatrix}$$

Rotation $R_Y(\theta)$ par rapport à l'axe Y de la sphère de Bloch

$$R_Y(\theta) = e^{-i\theta/2Y} = cos(\theta/2).\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} - i.sin(\theta/2)\begin{pmatrix}0 & i\\i & 0\end{pmatrix} = \begin{pmatrix}cos(\theta/2) & -sin(\theta/2)\\sin(\theta/2) & cos(\theta/2)\end{pmatrix}$$

Rotation $R_Z(\theta)$ par rapport à l'axe Y de la sphère de Bloch

$$R_Z(\theta) = e^{-i\theta/2Z} = cos(\theta/2).\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} - i.sin(\theta/2)\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = \begin{pmatrix}e^{-i\theta/2} & 0\\0 & e^{i\theta/2}\end{pmatrix}$$

Porte de déphasage

Les rotations selon l'axe Z correspondent à un changement de phase.
Les portes de déphasage sont synonymes des portes $R_Z(\theta)$, elles sont relativement simples à construire dans différentes technologies de qubits, on le trouve donc souvent dans les algorithmes.

- le qubit $|0\rangle$ devient $0\rangle$, qui est invariant, soit $R_\phi|0\rangle = |0\rangle$
- le qubit $|1\rangle$ subit un décalage de phase de ϕ, il devient $e^{i\phi}|1\rangle$, soit $R_\phi|1\rangle = e^{i\phi}|1\rangle$

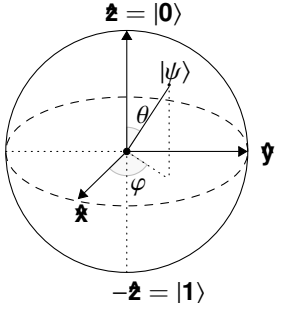
Cette porte modifie la phase entre la composante selon $|0\rangle$ et la composante selon $|1\rangle$

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Cette formulation est différente de celle de $R_Z(\phi)$ à un facteur $e^{-i\phi/2}$ près. Or on a vu que ce type de facteur n'a aucun impact sur la mesure, ces deux types de portes sont donc rigoureusement équivalents.

Groupe de Pauli

Si l'on considère la sphère de Bloch on peut remarquer que les opérateurs de Pauli X, Y et Z permettent de "sauter"entre les six points remarquables de la sphère.



En d'autres termes, l'identité et les portes de Pauli, soit l'ensemble $\{I, X, Y, Z\}$, muni de la multiplication matricielle, engendre un groupe dont la structure est assez triviale et qui se compose des 16 éléments $\{\pm I, \pm iI, \pm X, \pm iX, , \pm Y, \pm iY, \pm Z, \pm iZ\}$

Portes S et T

La porte S est la racine carrée de la porte Z.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

La porte S induit un déphasage de $\pi/2$ sur la composante $|1\rangle$ puisque $i = e^{i\pi/2}$

La porte T est la racine carrée de la porte S.

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

La porte S induit un déphasage de $\pi/4$ sur la composante $|1\rangle$

Groupe de Clifford

Le groupe de Pauli permet de "sauter" entre différents points remarquables de la sphère de Bloch, mais il est vite limité.

Il est plus intéressant de s'occuper du groupe formé par les portes de Clifford, ou groupe de Clifford. Celui-ci est généré par les portes H, CNOT et T. On s'intéressera aussi à la porte S qui est le carré de la porte T utilisée dans le théorème de Solovay-Kitaev

Construire les portes à 1 qubit

Il est trivial de définir une porte à un qubit mathématiquement, il suffit d'écrire une matrice unitaire de $\mathbb{C}^{2\times 2}$.

Les choses sont plus compliquées dans la réalité et dans le cadre d'une mise en œuvre industrielle. Comment peux-t'on construire toutes les portes possibles en n'utilisant qu'un nombre restreint de portes comme "briques de base" ?

La réponse est apportée par le théorème de Solovay-Kitaev.

Théorème de Solovay-Kitaev

Si dispose de la porte T et et la porte H, on peut construire une suite convergente de portes $P_n = A_n \times P_{n-1}$ où A_n est soit le produit $THTH$, soit le produit $HTHT$

En choisissant bien les différentes valeurs des A_n, on peut faire converger cette suite vers n'importe quel opérateur unitaire, donc vers n'importe quelle porte à un qubit.

En d'autres termes, on peut choisir ϵ aussi petit que l'on veut et trouver une composition de portes THTH et HTHT située à une distance inférieure à ϵ de la solution recherchée sur la sphère de Bloch.

À un facteur de précision ϵ près, on peut construire toutes les portes en ne sachant implémenter que H et T.

Décomposition ABC des portes à 1 qubits

Soit U une porte sur 1 qubit, il est possible de trouver 4 angles $(\alpha, \beta, \gamma, \delta]$ (qui représentent les quatre degrés de liberté de l'opérateur) tels que

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta+\delta}{2}} cos(\frac{\gamma}{2}) & -e^{-i\frac{\beta-\delta}{2}} sin(\frac{\gamma}{2}) \\ e^{i\frac{\beta-\delta}{2}} sin(\frac{\gamma}{2}) & e^{i\frac{\beta+\delta}{2}} cos(\frac{\gamma}{2}) \end{pmatrix}$$

On peut dès lors écrire U sous la forme suivante

$$U = e^{i\alpha} AXBXC$$

$$A \equiv e^{-\frac{i}{2}\beta Z} e^{-\frac{i}{4}\gamma Y}$$

$$B \equiv e^{\frac{i}{4}\gamma Y} e^{\frac{i}{4}(\beta+\delta)Z}$$

$$C \equiv e^{\frac{i}{4}(\beta-\delta)Z}$$

où X, Y et Z sont les opérateurs de Pauli, leurs exponentiels complexes représentent donc des rotations autour des axes correspondant dans la sphère de Bloch.

Remaqrque importante $ABC = I$

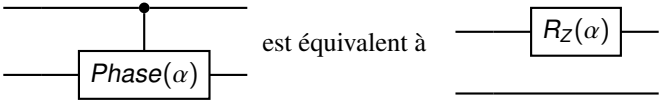
Déphasage contrôlé

ATTENTION : L'opérateur $Phase(\alpha)$ affecte à la fois la phase de $|0\rangle$ et $|1\rangle$, à ne pas confondre avec $R_Z(\alpha)$ qui n'affecte que la phase selon $|0\rangle$.

L'opérateur "$Phase(\alpha)$ contrôlé" correspond à $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Phase(\alpha)$

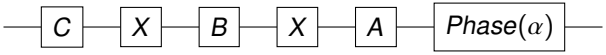
$$Phase(\alpha) = e^{i\alpha} \times I = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \text{ donc } CPhase(\alpha) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On déduit de l'équation précédente que

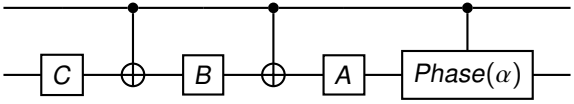


Construire une porte contrôlée sur 2 qubits 1/2

Soit un opérateur unitaire $U = e^{i\alpha} AXBXC$ avec $ABC = I$

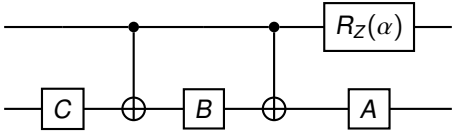


On construira CU en remplaçant les portes X par des CNOT et le déphasage par un déphasage contrôlé



Construire une porte contrôlée sur 2 qubits 2/2

Ce circuit est équivalent à

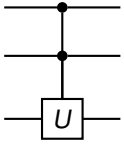


Ce circuit implémente bien CU, en effet

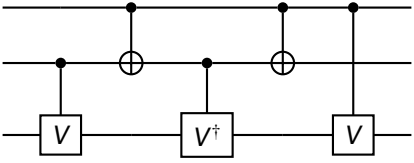
- si le qubit de contrôle vaut $|1\rangle$, on applique $e^{i\alpha}AXBXC$ sur le second, donc U
- si le qubit de contrôle vaut $|0\rangle$, on applique simplement ABC sur le second, donc on ne change rien puisque $ABC = I$

Porte à double contrôle - réduction de Sleathor-Weinfurter

Soit U un opérateur unitaire, soit V l'opérateur unitaire tel que $V^2 = U$, alors le circuit



Peut s'écrire sous la forme



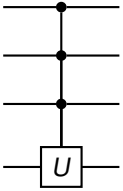
Réduction de Sleathor-Weinfurter - discussion

- si le premier qubit vaut $|0\rangle$ il ne change pas l'état du second qubit et,
  - si le second qubit vaut $|0\rangle$, aucune porte V n'est active sur le troisième qubit qui reste inchangé
  - si le second qubit vaut $|1\rangle$, il va activer les deux premières portes contrôlées sur le troisième qubit qui va subir $V \times V^\dagger = I$, donc ce dernier ne change pas ;
- si le premier qubit vaut $|1\rangle$, il active les portes CNOT sur le second qubit et la dernière contrôlée porte sur troisième qubit
  - si le second qubit vaut $|0\rangle$, il n'active pas la première porte, il passe à $|1\rangle$ à cause de la première porte CNOT, active la porte $V^\dagger$ sur le troisième qubit qui subit également une porte contrôlée V activée par le premier qubit, il subit $V \times V^\dagger = I$ et ne change donc pas
  - si le second qubit vaut $|1\rangle$, il active la première porte V, est retourné par le premier CNOT, passe à $|0\rangle$ et donc n'active pas $V^\dagger$, le troisième qubit subit également une porte V activée par le premier qubit, il subit donc $V \times V = V^2 = U$

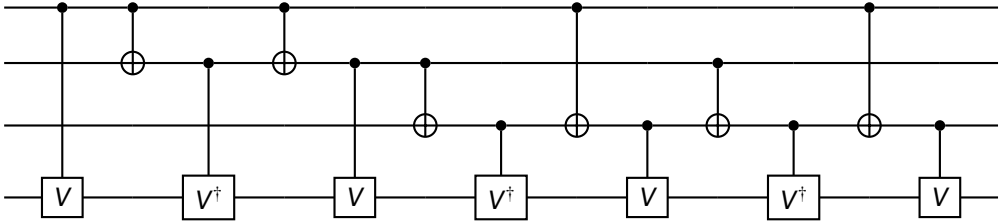
On voit donc que le troisième qubit subit l'effet d'une porte U (de deux portes V) avec double contrôle.

Toujours plus fort : triple contrôle !

Soit U un opératzeur unitaire et soit V l'opérateur unitaire tel que $V^4 = U$, alors

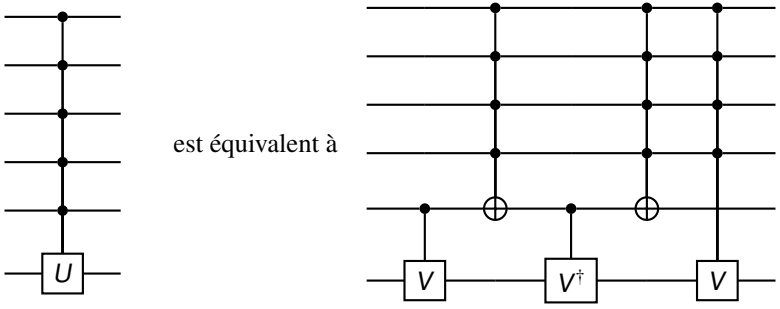


est équivalent à



Vers l'infini et au-delà ! Sleathor-Weinfuter revisité

Si U est unitaire et si V est sa racine carrée, alors



Il suffit de savoir construire des racines carrées et des portes N à contrôles multiples.

Une boite à outils universelle pour construire les portes quantiques

En conclusion, nous avons vu que

- on sait construire toutes les portes à un qubit à la précision ϵ près, via la méthode de Solovay-Kitaev
- la décomposition ABC et l'existence des portes CNOT, nous permet de consruire des portes contrôlés à 2 qubits
- la décomposition de Sleathor-Weinfurter permet de construire des portes à trois qubits, en par récurrence à autant de qubits de contrôle que l'on veut. On peut donc construire de portes NOT contrôlées par autant de qubits que l'on veut
- avec des CNOT à contrôle multiples et les racines carrées de portes, on peut construire des portes avec autant de qubits de contrôle que l'on veut

Par conséquent, il suffit de savoir implémenter physiquement les H, T et CNOT pour implémenter n'importe quelle porte à *n* qubits. Donc n'importe quel circuit.

ATTENTION : Cela peut nécessiter un **très** grand nombre de portes.

Algorithme de Shor - Introduction

L'algorithme de Shor est une pierre angulaire de la programmation quantique. Il est théoriquement capable de casser des chiffrements de type RSA, sur lesquels se basent les protocoles de sécurité d'Internet.

L'algorithme de Shor a largement contribué à la mise en lumière des principes et des ambitions de l'informatique quantique.
Nous allons voir

- quelques rappels sur le fonctionnement de RSA
- rappels sur la transformation de Fourier discrète (ou DFT)
- la QFT, l'implémentation quantique de la DFT
- l'algorithme de Simon
- l'algorithme de Shor qui utilise conjointement la QFT et l'algorithme de Simon..

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Rappel sur la base de Bell

Etabt donné le circuit qui construit la porte EPR, celui-ci envoie la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ sur la base suivante

- l'état $|00\rangle$ est envoyé sur la paire EPR, $|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- l'état $|01\rangle$ est envoyé sur $|\Psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- l'état $|10\rangle$ est envoyé sur $|\Phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- l'état $|11\rangle$ est envoyé sur $|\Psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

La situation

Est-il possible de déplacer un état entre deux acteurs et ainsi d'utiliser un circuit quantique pour transmettre de l'information sous la forme d'un qubit ?
Alice et Bon possède chacun un qubit de la paire EPR $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
Afin de partager plus d'information, Alice et Bob vont partagé un troisième qubit $|\phi\rangle$, non intriqué la paire EPR. Cet état est $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Le système est donc dans un état global $|\chi\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Astuce de calcul

On va ici avoir recours à une petite astuce de calcul : on ne mesurera pas la paire EPR dans la base canonique, mais dans la base constituée par les états de Bell. On va donc réécrire cet état dans cette nouvelle base (et ce qui suit n'est que du pur calcul algébrique).

Le calcul

On remarque que $|00\rangle|1\rangle = |001\rangle = |0\rangle|01\rangle$. On va donc avoir

$$\begin{aligned}|\chi\rangle &= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|111\rangle \\ &= \frac{\alpha}{\sqrt{2}}|00\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|01\rangle|1\rangle + \frac{\beta}{\sqrt{2}}|10\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|11\rangle|1\rangle\end{aligned}$$

Suite du calcul

Maintenant qu'on a fait apparaître l'ensemble des vecteurs de la base canonique, on transpose l'état dans la base de Bell en remplaçant les vecteurs canoniques par leurs expressions dans cette autre base .

$$
\begin{aligned}
|\chi\rangle &= \frac{\alpha}{\sqrt{2}}|00\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|01\rangle|1\rangle + \frac{\beta}{\sqrt{2}}|10\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|11\rangle|1\rangle \\
&= \frac{\alpha}{\sqrt{2}}\frac{1}{\sqrt{2}}(|\Phi+\rangle + |\Phi-\rangle)|0\rangle + \frac{\alpha}{\sqrt{2}}\frac{1}{\sqrt{2}}(|\Phi+\rangle - |\Phi-\rangle)|0\rangle + \\
&\frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}(|\Psi+\rangle + |\Psi-\rangle)|0\rangle + \frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}(|\Psi+\rangle - |\Psi-\rangle)|1\rangle \\
&= \frac{1}{2}[|\Phi+\rangle(\alpha|0\rangle + \beta|1\rangle)] + \frac{1}{2}[|\Phi-\rangle(\alpha|0\rangle - \beta|1\rangle)] + \\
&\frac{1}{2}[|\Psi+\rangle(\beta|0\rangle + \alpha|1\rangle)] + \frac{1}{2}[|\Psi-\rangle(\beta|0\rangle - \mathit{alpha}|1\rangle)]
\end{aligned}
$$

Constat

En résumé, on voit que $|\chi\rangle$ s'écrit avec 4 composantes dans la base de Bell :

$$
\begin{aligned}
|\chi\rangle &= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{2}[|\Phi+\rangle(\alpha|0\rangle + \beta|1\rangle)] + \quad (1) \\
&\frac{1}{2}[|\Phi-\rangle(\alpha|0\rangle - \beta|1\rangle)] + \quad (2) \\
&\frac{1}{2}[|\Psi+\rangle(\beta|0\rangle + \alpha|1\rangle)] + \quad (3) \\
&\frac{1}{2}[|\Psi-\rangle(\beta|0\rangle - \alpha|1\rangle)] \quad (4)
\end{aligned}
$$

Bilan

Si Alice effectue une mesure des deux premiers qubits dans la base de Bell, elle va mesurer chacun des états de Bell avec une probabilité de 25%, et le dernier qubit va s'effondrer sur l'un des quatre états possibles. Ces états ressemblent à $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ à une ou deux transformations unitaires près :

- si Alice mesure $|\Phi+\rangle$, on est dans le cas *(1)*, il n'y a rien à faire sur le dernier qubit pour mesurer $|\phi\rangle$
- si Alice mesure $|\Phi-\rangle$, on est dans le cas *(2)*, il faut changer le signe de la composante sur $|1\rangle$, ce qui se fait en applicant une porte Z
- si Alice mesure $|\Psi+\rangle$, on est dans le cas *(3)*, il faut interchanger permuter les deux coefficients, ce qui se fait avec une porte X
- si Alice mesure $|\Psi-\rangle$, on est dans le cas *(4)*, il faut changer le signe et ensuite permuter les coefficients, donc appliquer une porte Z puis une porte X, ce qui revient à appliquer un opérateur composé XZ

Beam me up, Scotty !

e son côté, Bob va lui aussi faire une mesure dans la base de Bell des deux premiers qubits et il obtiendra la même mesure qu'Alice, il saura donc quelle transformation appliquer parmi I, X, Z ou XZ et il obtiendra l'état $|\phi\rangle$.
On a donc déplacé l'état $|\phi\rangle$ du premier qubit au troisième qubit, mais au prix d'une mesure et de la destruction (et l'effondrement) de l'état du premier qubit. Ce n'est donc pas en contradiction avec le théorème de non-clonage. Ce phénomène constitue la téléportation quantique.

Codage super-dense

Bob peut éviter de mesurer les deux premiers qubits si Alice lui transmet (par des moyens non quantiques) deux bits a et b (de vrais bits, pas des qubits). Ces deux qubits décrivent lequel des quatre cas a été vu par Alice dans sa mesure. Bon n'a plus qu'à appliquer $X^a Z^b$ pour obtenir $|\phi\rangle$ sur le troisième qubit, attendu que $X^0 = Z^0 = I$. On parle alors de codage super-dense, trois qubits et deux bits standards permettent de déplacer un état quantique d'un qubit à l'autre.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Groupes multiplicatifs

RSA repose sur des fondements arithmétiques. Soit $N = p.q$ le produit de deux (grands) nombres premiers p et q.

On définit l'ensemble $\mathbb{Z}/N\mathbb{Z}$, l'ensemble des entiers modulo N, dont le cardinal est N. Si N était premier, cet ensemble serait un groupe multiplicatif (ce n'est pas le cas ici).

On définit l'ensemble $(\mathbb{Z}/N\mathbb{Z})*$ le sous-ensemble de $\mathbb{Z}/N\mathbb{Z}$ des nombres qui sont premiers avec N. Cet ensemble est un groupe multiplicatif.

Indicatrice d'Euler

Le cardinal de $(\mathbb{Z}/N\mathbb{Z})*$ est appelé *indicatrice d'Euler* de N, elle est notée $\Phi(N)$. L'indicatrice d'Euler donne le nombre d'entiers qui sont premiers avec N.

Dans le cas où $N = p.q$ avec p et q premiers, on peut montrer que $\phi[N] = (p-1)(q-1)$

L'indicatrice d'Euler est associée au **théorème d'Euler**

$$\forall a \in \mathbb{N}, \forall n \in \mathbb{N}, n > 0, \text{ a premier avec n }, a^{\phi(n)} \equiv 1[n]$$

Si a et n sont premier entre eux, alors élevé à la puissance $\phi[n)$ est congruent à 1 modulo n.

Le fonctionnement de RSA

On choisit deux entiers e et d tels que $e.d = 1$ modulo $\phi[N]$, e premier avec $\phi[N]$. Le nombre d est l'inverse de e dans $(\mathbb{Z}/N\mathbb{Z})*$

On construit les clefs privées et publiques de la façon suivante :

- la clef publique est le produit $N.d$
- la clef privée est le produit $N.e$

Supposons que Alice veuille envoyer l'entier P à Bob. Alice construit le chiffrement C défini par $C = P^e(modN)$.

La magie de RSA, ce résume dans cette formule : $C^d(modN) = P$, on chiffre connaissant e, on déchiffre connaissant d.

RSA - Démonstration

Sachant que $e.d = 1[\phi[N)]$, $\exists k, e.d = k\phi(N) + 1$, et donc $\phi[N) = (p-1)(q-1)$.

Il est toujours possible de choisir N, p, q de telle sorte qu'ils soient grands par rapport à P. En fait, on découpe le message à envoyer en tronçons qui sont assez petits pour être plus petit que p et q, et donc d'être premier avec N. Par conséquent, d'après le théorème d'Euler, pour tout entier P, $P^{\phi(N)} = 1[N]$

$$C^d[N] = P^{e.d}[N] = P^{k\phi(N)+1)}[N] = P.P^{k\phi(N)}[N] = P.(P^{\phi(N)})^k = P.1^k[N] = P[N]$$

En conclusion, en découpant le message en entiers P suffisamment petits, si Alice et Bon connaissent leurs clefs publiques respectives et leurs propres clefs secrètes, et peuvent chiffrer et déchiffrer P.

L'algorithme de Shor fragilise RSA

Pour casser RSA, il faut pouvoir calculer d connaissant e et N, donc il faut calculer l'indicatrice d'Euler qui est égale à $\phi(N) = (p-1)(q-1)$, il faut donc calculer p et q, donc factoriser $N = p.q$.

L'algorithme de Shor permet de faire cette factorisation dans une durée raisonnable, il affaiblit les bases mêmes de l'algorihme RSA.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Transformée de Fourier classique et DFT

S f est fonction du temps (exprimé en seconde) et ν représente une fréquence (exprimée en hertz) :

$$\hat{f}(\nu) = \int_{-\infty}^{+\infty} f(t) e^{-2i\pi\nu t}\, dt$$

Si $(s_n)_{0\leq n<N}$ est une suite de N valeurs, on définira sa transformée de Fourier discrète, ou **DFT**, comme la suite $(\hat{s}_n)_{0\leq n<N}$

$$0 \leq n < N, \hat{s}_n = \sum_{k=0}^{N-1} s_k . e^{-2i\pi \frac{kn}{N}}$$

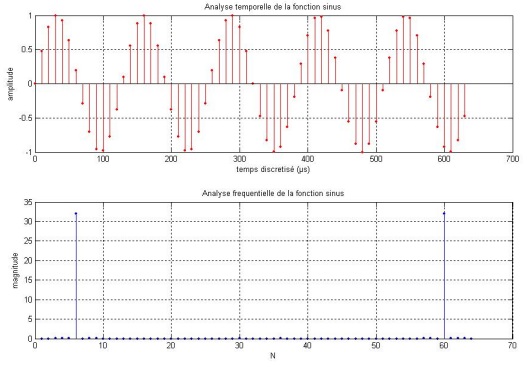
La suite $(\hat{s}_n)$ es la décomposition spectrale de la suite (s_n).

Si l'on pose $\omega_N^i = e^{-2i\pi\frac{1}{N}}$, la i$^{\text{ème}}$ racine N$^{\text{ème}}$ de l'unité, on peut écrire

$$\hat{s}_n = \sum_{k=0}^{N-1} s_k . \omega_N^{kn}$$

$$s_n = \frac{1}{N} \sum_{k=0}^{N-1} \hat{s}_k . \omega_N^{-kn}$$

Décomposition spectrale discrète



La décomposition spectrale est équivalente à la suite d'origine, on passe facilement de l'une à l'autre.

$$\hat{s}_n = \sum_{k=0}^{N-1} s_k.\omega_N^{kn}, \text{ et réciproquement } s_n = \frac{1}{N}\sum_{k=0}^{N-1} \hat{s}_k.\omega_N^{-kn}$$

Matrice de Vandermonde-Fourier

Connaissant les $\omega_N^i = e^{2i\pi\frac{1}{N}}$, on peut écrire la matrice suivante, dite *matrice de Vandermonde-Fourier*

$$W_N = (\omega_N^{(i-1)(j-1)})_{1\leq i,j\leq N} = \begin{pmatrix} 1 & 1 & 1 & \cdot & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

Opérateurs unitaires

La matrice de Vandermonde est presque unitaire (démonstration complète dans le poly), en effet

$$QF_N = \frac{1}{\sqrt{N}} W_N \text{ est unitaire mais non hermitienne}$$

A titre d'exmple on a

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ et } W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}$$

Au rang 2, la DFT se confond avec la porte de Hadamard.

Transformée de Fourier quantique

La transformée de Fourier quantique (ou QFT) est une implémentation de la DFT via des méthodes d'informatique quantique.

Soit $g()$ une fonction entière à valeurs dans $\mathbb{C}$.

$$g : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}$$

On peut construire le vecteur suivant

$$\frac{1}{\sqrt{2^n}} \begin{pmatrix} g((0) \\ g(1) \\ \vdots \\ g(2^n - 1) \end{pmatrix}$$

qui correspondant à l'état quantique normalisé $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$.
On dispose d'un isomorphisme canonique entre les états quantiques et ce type de fonctions.

QFT sous forme matricielle

$$QF_n = \frac{1}{\sqrt{N}} W_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdot & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

Exemple : Dans le cas où il y a 3 qubits, on aura la matrice 8×8 suivante

$$QF_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^1 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \text{ avec } \omega = e^{\frac{2i\pi}{8}}$$

Images des vecteur de la base canonique par la QFT

Puisque QF_n est unitaire, ses vecteurs propres forment une base orthonormée.

Les colonnes de cette matrice sont les images des vecteurs de la base canonique.

Ainsi si $|k\rangle$ est le k$^{\text{ème}}$ vecteur de la base canonique, son image par QF_n est

$$QF_n \times |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^n-1} \omega_{2^n}^{kj} |j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} |j\rangle$$

QFT sous forme de circuit quantique

On n'utilisera que deux types de portes :

- des portes de Hadamard pour créer un état de superposition uniforme ;
- des portes de phases contrôlées, notées RP_m, dont la phase aura la valeur $\frac{2\pi}{2^m}$

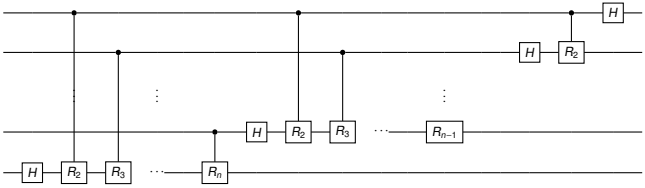


Figure – Circuit implémentant une QFT

Autre écriture mathématique de la QFT

On peut démontrer que la QFT, définie par

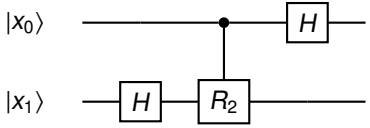
$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{kj}{2^n}} |j\rangle$$

est équivalente à la forme suivante (démonstration complète dans le poly).

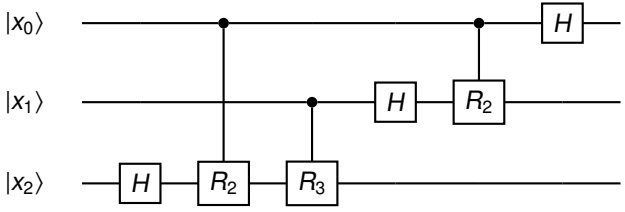
$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{j=1}^{n} (|0\rangle + e^{2i\pi \frac{k}{2^j}} |1\rangle)$$

$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2i\pi \frac{k}{2}} |1\rangle) \otimes (|0\rangle + e^{2i\pi \frac{k}{2^2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2i\pi \frac{k}{2^n}} |1\rangle) \otimes$$

Premiers cas simples



On sait construire les QFT pour n'importe quel nombre n de qubits, par récurrence.



Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Introduction

Daniel Simon a décrit l'algorithme qui porte son nom en 1997. Celui-ci permet de déterminer la période d'une fonction booléenne périodique. Cet algorithme exploite une nouvelle idée, à savoir l'effondrement causé par la mesure d'un état.

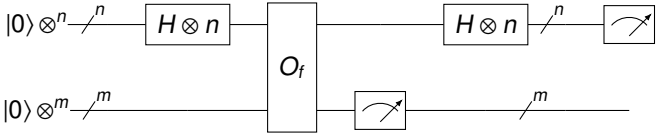
L'algorithme de Simon sert de base à l'algorithme de Shor.

Remarque préalable : une fonction périodique booléenne qui a N arguments possible prend exactement N valeurs. En effet, si f est L-périodique, alors $f(x) = f(x \oplus L) = f(x \oplus L \oplus L)$.

Avec n bits, le cardinal de $\{0,1\}^n$ est 2^n. Il faut faire des tirage de x et de calcul de $f(x)$ et s'arrêter lorsque l'on voit pour la seconde fois une valeur $f(x)$ que l'on a déjà vue. Dans le cas le plus défavorable, il faudra effectuer $2n - 1 + 1$ tirages pour être sûr de faire un tel tirage et de deviner ainsi la période.

Approche quantique

Le circuit qui implémente l'algorithme de Simon exploite n qubits et m acillae.



La bordée initiale de portes H produit une superposition uniforme sur les n qubits de données.

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \, |0\rangle^{\otimes m}$$

Lorsqu'on applique l'oracle qui évalue $f()$ sur la superposition via les ancillae

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \, \big|f(x)\big\rangle$$

Impact de la mesure dans le calcul

L'astuce de cet algorithme, c'est d'exploiter l'effondrement quantique consécutif à une mesure

- On effectue une mesure des m ancilla
- cela revient à choisir une valeur $f(a)$ arbitrairement
- comme la fonction est booléenne et L-périodique, les seuls états qui subistent en superposition après l'effondrement causé par la mesure sont $|a\rangle$ et $|a \oplus L\rangle$ puisque $f(a) = f(a \oplus L)$

Juste après la mesure, on aura donc l'état suivant :

$$\frac{1}{\sqrt{2}}(|a\rangle + |a \oplus L\rangle)\left|f(a)\right\rangle)$$

Hadamard entre dans la danse

On applique n portes de Hadamard, comme dans l'algorithme de Bernstein-Vazirini.
On rappelle que

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^{n-1}} (-1)^{x \cdot y} |y\rangle$$

Appliqué à l'état précédent

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}(|a\rangle + |a+L\rangle)\big|f(a)\rangle\right)) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} ((-1)^{a \cdot y} + (-1)^{(a \oplus L) \cdot y})\,|y\rangle$$

qui peut être écrit

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{a \cdot y}(1 + (-1)^{s \cdot y})\,|y\rangle$$

Discussion

Considérons l'équation obtenue

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{a \cdot y} (1 + (-1)^{L \cdot y}) \, |y\rangle$$

- si $s \cdot y = 1$, on a ajoute 1 et -1 et ont contribue pour 0 ;
- si $s \cdot y = 0$, on ajoute des contributions qui subsistent.

Il ne subsiste dans l'état que les composantes telles que $L \cdot y = 0$.
On a donc sur les n premiers qubits une superposition d'états $|y\rangle$ tels que $L \cdot y = 0$.

Si on fait une mesure, on va découvrir l'un de ces états. On ne connaîtra pas L de manière explicite, on va connaître une variable dont le produit pointé avec L donne 0.

Multiples tirages et systèmes linéaires

On va effectuer plusieurs tirs et construire une suite (y_i) qui vérifie $\forall i, y_i \cdot L = 0$
Avec k tirages on construit le système d'équations linéaires :

$$\begin{cases} y_1 \cdot L = 0 \\ y_2 \cdot L = 0 \\ \vdots \\ y_k \cdot L = 0 \end{cases}$$

On peut démontrer qu'avec $n - 1$ tirages, la probabilité d'avoir un système d'équations indépendantes, qui permette de trouver la valeur de s, est de 25%.
En réalisant au plus $4n$ tirages, on est sûr d'avoir un système qui permette de connaître s.

On trouve la solution en $4n$ étapes au plus, une approche classique aurait nécessité 2^{n-1} au plus.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Arithmétique modulo n

L'algorithme de Shor combine habilement la QFT et les idées de l'algorithme de Simon. Shor s'intéresse à l'arithmétique modulo n.

Si $n \in \mathbb{Z}$, on notera $\mathbb{Z}/n\mathbb{Z}$ le groupe quotient défini par la relation d'équivalence "a le même reste lors d'une division entière par n".
Si n est un nombre premier, alors $\mathbb{Z}/n\mathbb{Z}$ est un corps fini, puisque c'est un anneau quotienté par l'un de ses idéaux premiers.

On notera $(\mathbb{Z}/n\mathbb{Z})^*$ la sous-partie de $\mathbb{Z}/n\mathbb{Z}$ qui ne comprend que les éléments qui sont premiers avec n, c'est-à-dire qui n'ont pas de facteurs premiers communs avec n.

On peut montrer que $(\mathbb{Z}/n\mathbb{Z})^*$ forme un groupe fini vis-à-vis du produit, en d'autre termes

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*, \exists b \in (\mathbb{Z}/n\mathbb{Z})^*, x \times b = 1[n]$$

Il est légitime dès lors de parler d'élévation à la puissance dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Bases mathématiques de l'algorithme de Shor

Soit N un entier que l'on souhaite factoriser. Soit a un entier plus petit que $\sqrt{N}$

L'idée de base de l'algorithme de Shor consiste à rechercher les valeurs r telles que

$$a^r \equiv 1[N], \text{c'est à dire } a^r = 1 \text{ dans } (\mathbb{Z}/n\mathbb{Z})^*$$

Décrivons la fonction f_a suivante :

$$f_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z}^*), f_a : x \mapsto a^x$$

Si r est tel que $a^r \equiv 1[N]$ alors pour tout p, on a $a^{r+p} = a^r.a^p = a^p$ ce qui revient à dire que $f_a(r+p) = f_a(p)$ donc que f_a admet une période r.

Inversement, si on découvre une valeur r telle que f_a est$r$-périodique, alors on a trouvé une valeur r telle que $a^r \equiv 1[N]$.

Intérêt de trouver une puissance périodique

Si cette valeur r est impaire, on ne peut rien en faire, mais si r est paire, on peut trivialement trouver p tel que $r = 2p$.

On sait depuis longtemps que $x^2 - 1 = (x-1)(x+1)$, par conséquent

$$\text{Si } a^r \equiv 1[N], r = 2p, a^{2p} - 1 = (a^p - 1)(a^p + 1) = 0 \text{ dans } (\mathbb{Z}/n\mathbb{Z})^*$$

Si l'on sort de $(\mathbb{Z}/n\mathbb{Z})^*$, cela signifie que

$$\exists k \in \mathbb{N}, (a^p - 1)(a^p + 1) = kN$$

Cela signifie que les facteurs premiers de N sont répartis entre $a^p - 1$ et $a^p + 1$.

Calculer le PGCD est trivial, par exemple en utilisant l'algorithme d'Euclide. Il suffit dès que de calculer $PGCD(a^p - 1, N)$ et $PGCD(a^p + 1, N)$ pour trouver les facteurs recherchés.

Un exemple trivial, mais concret

Supposons que 15 soit un nombre très difficile à factoriser, et appliquons la recette précédente. On a donc $N = 15$.

Prenons un nombre a inférieur 15, par exemple $a = 7$, et évaluons $f(a) = 7^a[15]$.

a	7^a	f(a)
1	7	7
2	49	4
3	343	13
4	2401	1

On s'arrête ici car $7^4 = 1[15]$, et en plus 4 est le double de 2 ! ! !

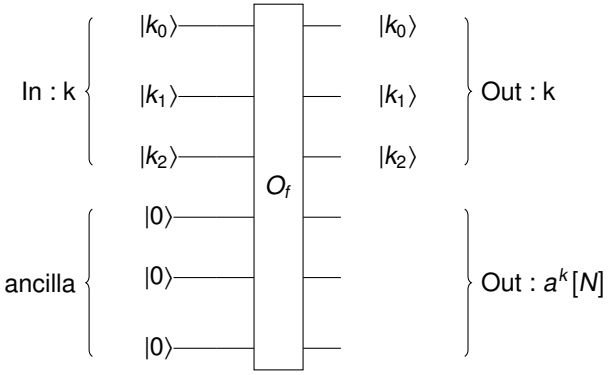
Dès lors, on calcule $PGCD(7^2 + 1, 15) = PGCD(50, 15) = 5$ et $PGCD(7^2 - 1, 15) = PGCD(48, 15) = 3$.

On sait maintenant que $15 = 3 \times 5$!

Implémentation quantique de Shor

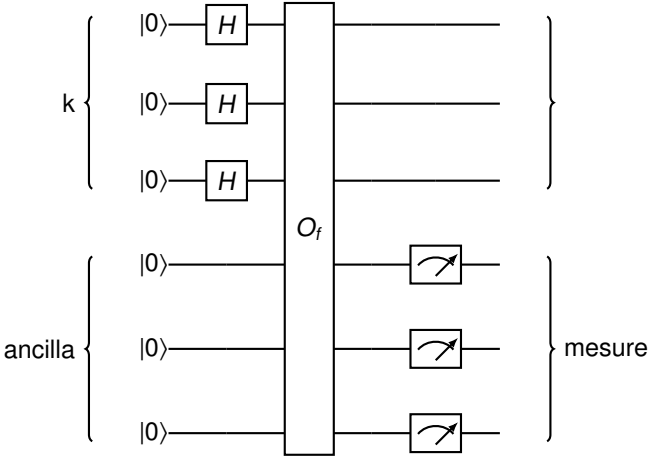
On souhaite factoriser l'entier N, on a n qubits et $2^n \geq N$, soit $a < N$

Les qubits d'entrées représentent la valeur k sous forme binaire, ses bits sont k_0, k_1, ..., k_p.
L'action de l'oracle transforme $|k\rangle \otimes |0\rangle$ en $|k\rangle \otimes \left|a^k\right\rangle$



183/370

Première étape du circuit



Calcul de l'état du système après la première étape 1/2

L'état initial est $|\phi_0\rangle = |0\cdots0\rangle \otimes |0\cdots0\rangle$, l'application de n portes de Hadamard va le changer en $|\phi_1\rangle$

$$|\phi_1\rangle = (H^{\otimes n} \otimes I)\,|\phi_0\rangle = (H^{\otimes n} \otimes I) \times (|0\rangle \otimes |0\rangle) = (\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |0\rangle$$

Si on applique l'oracle qui implémente f, on obtient alors $|\phi_2\rangle$

$$|\phi_2\rangle = O_f((\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes \left|a^k\right\rangle$$

On a choisit la valeur a au hasard. On vérifie rapidement (algorithme d'Euclide) que a est premier avec N. Si a n'est pas premier avec N... on vient de trouver un diviseur de N ! On s'arrête là le problème est résolu.

185/370

Ce que l'on va faire avec l'algorithme

Soit r la période recherchée, on a

$$\forall p, a^{p+r} \equiv a^p[N] \text{ et donc } a^r \equiv 1[N]$$

Pour chaque entier k, on peut écrire $k = pr + q, 0 \leq q < r$, donc

$$|k\rangle \otimes \left|a^k\right\rangle = |pr+q\rangle \otimes \left|a^{pr+q}\right\rangle = |pr+q\rangle \otimes \left|a^q\right\rangle \text{ car } a^r \equiv 1[N]$$

On peut dès lors réécrire $|\phi_3\rangle$

$$\begin{aligned}
|\phi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes \left|a^k\right\rangle &= \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \sum_{p=0}^{(2^n/r)-1} |pr+q\rangle \otimes \left|a^{pr+q}\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \sum_{p=0}^{(2^n/r)-1} |pr+q\rangle \otimes \left|a^q\right\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \Big(\sum_{p=0}^{(2^n/r)-1} |pr+q\rangle \Big) \otimes \left|a^q\right\rangle
\end{aligned}$$

Mesure des ancillae

Comme dans l'algorithme de Simon, on effectue une mesure des qubits ancillaires. L'état $|\phi_3\rangle$ s'effondre sur un état $|\phi_4\rangle$ qui correspond à un certain q_0 dont on sait simplement qu'il est inférieur à r.

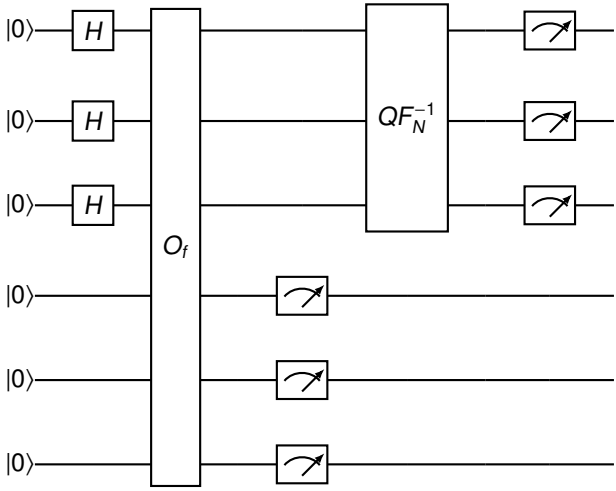
$$|\phi_4\rangle = \frac{\sqrt{r}}{\sqrt{2^n}}\left(\sum_{p=0}^{(2^n/r)-1} |pr + q_0\rangle\right) \otimes \left|a^{q_0}\right\rangle$$

La mesure des premiers qubits permet de connaître l'une des valeurs $|pr + q_0\rangle$.

On ne connaît pas r (la valeur que l'on cherche), et on ne peut pas déterminer p. On ne dispose de rien d'utile.

La QFT entre en scène

On vient compléter le circuit avec une QFT **inversée**



Effets de la QFT inversée

On rappelle que

$$QF_N^{-1} \times |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{-jk} |j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2i\pi \frac{jk}{N}} |j\rangle$$

La QFT inversée appliquée sur $|\phi_4\rangle$ donne le résultat $|\phi_5\rangle$ suivant

$$|\phi_5\rangle = (QF_N^{-1} \otimes I) \times |\phi_4\rangle = (QF_N^{-1} \otimes I) \times (\frac{\sqrt{r}}{\sqrt{2^n}} (\sum_{p=0}^{(2^n/r)-1} |pr + q_0\rangle) \otimes |a^{q_0}\rangle$$

$$= \frac{\sqrt{r}}{\sqrt{2^n}} (\sum_{p=0}^{(2^n/r)-1)} QF_N^{-1} \times |pr + q_0\rangle) \otimes |a^{q_0}\rangle$$

$$= \frac{\sqrt{r}}{\sqrt{2^n}} (\sum_{p=0}^{(2^n/r)-1)} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{N-1} e^{-2i\pi \frac{j(pr+q_0)}{N}} |j\rangle) \otimes |a^{q_0}\rangle$$

$$= \frac{\sqrt{r}}{2^n} (\sum_{j=0}^{N-1} \sum_{p=0}^{(2^n/r)-1} e^{-2i\pi \frac{j(pr+q_0)}{N}} |j\rangle) \otimes |a^{q_0}\rangle$$

$$= \frac{\sqrt{r}}{2^n} (\sum_{j=0}^{N-1} (\sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p \frac{jr}{2^n}}) e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle) \otimes |a^{q_0}\rangle$$

189 / 370

Simplification de l'équation

La situation est analogue à Bernstein-Vazirini : on ne le voit pas, mais beaucoup de termes sont en fait nuls !
Intéressons-nous au terme $e^{-2ip\pi\frac{jr}{2^n}}$) et à la somme de ces termes :

- si $\frac{jr}{2^n}$ est un entier, on élève $e^{-2i\pi} = 1$ à la puissance et on fait en fait une somme de 1 ;
- si $\frac{jr}{2^n}$ n'est pas un entier, on a une série géométrique de raison $e^{-2i\pi\frac{jr}{2^n}}$)

Rappel mathématique : On dispose du résultat suivant sur les suites

$$\forall k \neq 1, 1 + k + k^2 + k^3 + \cdots + k^{N-1} = \sum_{p=0}^{N-1} k^p = \frac{1 - k^N}{1 - k}$$

Termes nuls et termes non-nuls

On a donc deux cas. Dans le premier $\frac{jr}{2^n}$ est un entier et

$$\sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p \frac{jr}{2^n}} = \sum_{p=0}^{(2^n/r)-1} 1 = \frac{2^n}{r}$$

Dans le second cas $\frac{jr}{2^n}$ n'est pas un entier et

$$\sum_{p=0}^{2^n/(r-1)} e^{-2i\pi p \frac{jr}{2^n}} = \frac{1 - e^{-2i\pi \frac{jr}{2^n} \frac{2^n}{r}}}{1 - e^{-2i\pi \frac{jr}{2^n}}} = \frac{1 - e^{-2i\pi j}}{1 - e^{-2i\pi \frac{jr}{2^n}}} = \frac{1 - 1}{1 - e^{-2i\pi \frac{jr}{2^n}}} = 0$$

Donc seul le cas où $\frac{jr}{2^n}$ est un entier donne une contribution non nulle, ce qui simplifie $|\phi_5\rangle$

État final du circuit avant dernière mesure

$$|\phi_5\rangle = \frac{\sqrt{r}}{2^n}\Big(\sum_{j=0}^{N-1}\Big(\sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p\frac{jr}{2^n}}\Big)e^{-2i\pi\frac{q_0 j}{2^n}}|j\rangle\Big)\otimes\left|a^{q_0}\right\rangle = \frac{\sqrt{r}}{2^n}\Big(\sum_{j=0,\frac{jr}{2^n}\in\mathbb{N}}\frac{2^n}{r}e^{-2i\pi\frac{q_0 j}{2^n}}|j\rangle\Big)\otimes\left|a^{q_0}\right\rangle$$

$$= \frac{1}{\sqrt{r}}\Big(\sum_{j=0,\frac{jr}{2^n}\in\mathbb{N}} e^{-2i\pi\frac{q_0 j}{2^n}}|j\rangle\Big)\otimes\left|a^{q_0}\right\rangle$$

On réalise ici ne hypothèse simplificatrice : on suppose que la période recherchée r divise 2^n Dans ce cas, de 0 à $2^n - 1$, il y a r fois où $\frac{jr}{2^n}$ est entier, on change l'index précédent pour écrire l'état de la manière suivante

$$|\phi_5\rangle = \frac{1}{\sqrt{r}}\Big(\sum_{j=0,\frac{jr}{2^n}\in\mathbb{N}} e^{-2i\pi\frac{q_0 j}{2^n}}|j\rangle\Big)\otimes\left|a^{q_0}\right\rangle$$

$$= \frac{1}{\sqrt{r}}\Big(\sum_{l=0}^{r-1} e^{-2i\pi q_0\frac{l}{r}}\left|\frac{2^n l}{r}\right\rangle\Big)\otimes\left|a^{q_0}\right\rangle$$

192 / 370

Dernière mesure

Sous réserve de l'hypothèse ou r divise 2^n, on a

$$|\phi_5\rangle = frac1\ \sqrt{r}(\sum_{l=0}^{r-1} e^{-2i\pi q_0 \frac{l}{r}} \left|\frac{2^n l}{r}\right\rangle) \otimes \left|a^{q_0}\right\rangle$$

La mesure qui suit la QFT inverse va faire s'effondrer la superposition d'état vers l'un des états de bases qui la compose, on va voir un certain état $|\phi_6\rangle$

$$|\phi_6\rangle = \left|\frac{2^n l_0}{r}\right\rangle \otimes \left|a^{q_0}\right\rangle$$

Le circuit nous permet donc de connaître une valeur entière $\frac{2^n l_0}{r}$, mais pas encore la valeur de la période r que nous cherchons.

Récupération de la période - problématique

Supposons, après avoir divisé par 2n que l'on obtienne 0.5, a-t-onla fraction 1/2 (donc l = 1, r = 2), 2/4 (donc l = 2, r = 4) ou 4/8 (donc l = 4, r = 8) ?

Il est indispensable de lancer le circuit plusieurs fois pour avoir une série de couples (li, rj). Si l'on découvre un couple, (l1, r1) et (l2, r2) tels que r1 = r2 et si l1 et l2 sont premiers entre eux alors on peut conclure sur la valeur de r.

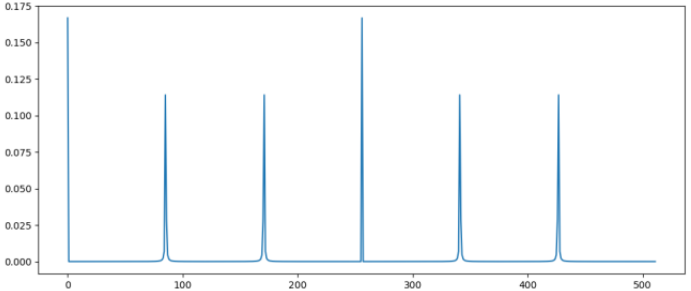
Par exemple, supposons qu'on ait échantillonné 3/8, 1/2, 7/8 . Les couples (3,8) et (7,8) nous permettent de conclure que $r = 8$.

Comme pour l'algorithme de Simon, il faut faire plusieurs runs du circuit pour conclure. On peut démontrer qu'il y a une probabilité supérieure à 5d'avoir deux l_i premiers entre eux, on est donc certain de trouver deux valeurs qui permettent de conclure avec 20 tirages

Retour sur l'hypothèse simplificatrice

On a supposé que r divise 2^n,et chaque cas $\left|\frac{2^n l_0}{r}\right\rangle$ sera présent $2^n/r$ fois.

Dans le cas où r ne divise pas 2^n, chque cas sera vu soit $\lfloor 2^n/r \rfloor$ fois, soit $\lceil 2^n/r \rceil$ fois. Les occurrences des valeurs possibles suivent une distribution qui ressemble à la figure suivante qui correspond au cas N=512 (9 qubits) et la période cherchée égale à 6.



195/370

Exploitation des fractions continues

Soit $s = \frac{2^n l_0}{r}$, la mesure effectuée, il est possible de trouver un entier d tel que

$$|s.r - d.N| \leq \frac{r}{2}$$

et donc

$$|\frac{s}{N} - \frac{d}{R}| \leq \frac{1}{2N} \leq \frac{1}{M^2}$$

La décomposition en fractions continues permet de conclure.

Entracte - éléments sur les fractions continues

Les fractions continues forment une nouvelle manière d'écrire des réels.
Une écriture décimale revient à écrire ceci :

$$x \in \mathbb{R}, x = x_0, x_1 x_2 x_3 \cdots, x = x_0 + \sum_{i=1}^{+\infty} x_k.10^{-k}$$

L'écriture en fractions continues revient à écrire ceci :

$$x \in \mathbb{R}, x = [x_0; , x_1, x_2, x_3, \cdots], x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}}$$

Certains nombres bien connus adoptent des décompositions en fractions continues simples :

- le nombre d'or ϕ est la racine positive de $X^2 = X + 1$, donc $\phi = 1 + \frac{1}{\phi}$ et sa décomposition en fractions continues est [1 ; 1, 1, 1, 1, ...] ;
- la racine de 2 vérifie $(\sqrt{2} - 1)(\sqrt{2} - 1) = 2 - 1 = 1$ donc $\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}}$, soit $\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}$ et sa décomposition en fractions continues est [1 ; 2, 2, 2, ...]

N-réduites d'une fraction continue

On peut utiliser les fractions continues pour construire des approximations de nombres dont on connaît la décomposition.
Si on a $a = [a_0; a_1, a_2, a_3, a_4, \cdots]$, on définit la **n-réduite** comme la décomposition arrêté au $n^{ème}$ terme.

Par exemple, on définit de la décomposition de π en fractions continues, soit [3 ; 7, 15, 1, 292, 1, 1, ...] les approximations 22/7 et 333/106 .

Identifier la période avec des fractions continues

Dans notre exemple, on a mesure $s = \frac{247}{512}$, on peut écrire

$$\frac{427}{512} = 0 + \frac{1}{\frac{512}{427}} = 0 + \frac{1}{1 + \frac{85}{427}}$$

Mais

$$\frac{85}{427} = \frac{1}{\frac{427}{85}} = \frac{1}{5 + \frac{2}{85}}$$

Et ainsi de suite... On en déduit la décomposition en fractions continues 427/512 = [0 ; 1, 5, 42, 2]. On calcule les différents n-réduites et on obtient 0, 1, 5/6, 211/253, 427/512.

On sait que la période est inférieur à M, donc à 21 dans notre cas, on retient donc l'approximation 5/6, la dernière à avoir un dénominateur acceptable .

On réalise plusieurs tirages jusqu'à avoir deux fractions qui ont le même dénominateur et des numérateurs premiers entre eux.

Plan

13 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
14 Premiers algorithmes quantique : Bernstein-Vazirini
15 Théorème de non-clonage
16 Boite à outils universelle pour construire les portes
17 Téléportation quantique et codage super-dense
18 Les mathématiques derrière RSA
19 Transformée de Fourier discrète et transformée de Fourier quantique
20 Algorithme de Simon
21 Algorithme de Shor
22 Algorithme de Grover

Que fait l'algorithme de Grover

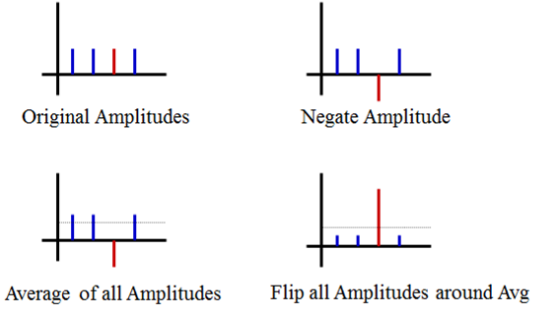
Supposons que l'on puisse ramener la résolution d'un problème à une fonction booléenne de n bits vers un seul bit telle que la fonction est nulle partout sauf sur la valeur des bits qui représente la solution.

L'algorithme de Grover permet de trouver rapidement le point k_0 tel que $f(k_0) = 1$ sans avoir à tester les 2^n valeurs possibles de la variable.

Par la magie de la superposition des états et des mesures multiples, il est possible d'étendre Grover si la fonction f est non nul en un faible nombre de points.

L'algorithme de Grover offre une performance en $0(\sqrt{n})$, on peut déémontrer qu'aucun algorithme ne pourra faire mieux qu'un gain quadratique. On doit cet algorithme à Lov Grover en 1996.

Grover dans les grandes lignes



Fonctionnement schématique

le schéma de fonctionnement est globalement le suivant :

1. on part de la superposition uniforme,
2. on applique un oracle spécial, ce qui rend négatif le terme k_0 ;
3. on réalise la moyenne de toutes les valeurs, celle -ci est inférieur à la moyenne de l'étape initiale puisqu'une valeur est négatiive ;
4. on inverse toutes les valeurs par rapport à cette moyenne, qui deviennent toutes supérieures à la moyenne calculée, cette opération fait ressortir davantage la valeur associée à k_0

Si itère ce processus plusieurs fois, on fait ressortir d'autant plus l'état qui correspond à k_0 dont la mesure devient de plus en plus probable.

Cette façon de procéder est appelée **amplification de phase**.

Oracle de Grover 1/3

Dans l'algoritme de Grover, il est utile de disposer d'un oracle dont le comportement est

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0. \end{cases}$$

Comment construire cet opérateur unitaire connaissant la fonction f et l'oracle O_f associé ? Prenons un oracle "classique",

$$f : \mathbb{B}^n \to \mathbb{B}$$

$$\forall x \neq x_0, f(x) = 0 \text{ mais } f(x_0) = 1 O_f : \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \to \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \, |x\rangle \, |y\rangle \mapsto |x\rangle \left|y \oplus f(x)\right\rangle$$

Oracle de Grover 2/3

On initialise l'ancilla à $|-\rangle$, c'est simple à faire en appliquant une porte X puis une porte H.
On remarque que $O \oplus x = x$ et $1 \oplus x = \neg x$

$$\begin{aligned} O_f(|x\rangle \otimes |-\rangle) &= \frac{1}{\sqrt{2}}(O_f(|x\rangle |0\rangle) - O_f(|x\rangle |1\rangle)) \\ &= \frac{1}{\sqrt{2}}(|x\rangle \left|0 \oplus f(x)\right\rangle - |x\rangle \left|1 \oplus f(x)\right\rangle) \\ &= \frac{1}{\sqrt{2}}(|x\rangle \left|f(x)\right\rangle - |x\rangle \left|\neg f(x)\right\rangle) \end{aligned}$$

$$\text{Si } f(x) = 0, O_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}}(|x\rangle \left|f(x)\right\rangle - |x\rangle \left|\neg f(x)\right\rangle) = \frac{1}{\sqrt{2}}(|x\rangle) |0\rangle - |x\rangle |1\rangle = |x\rangle |-\rangle$$

$$\text{Si } f(x) = 1, O_f(|x\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}}(|x\rangle \left|f(x)\right\rangle - |x\rangle \left|\neg f(x)\right\rangle) = \frac{1}{\sqrt{2}}(|x\rangle) |1\rangle - |x\rangle |0\rangle = -|x\rangle |-\rangle$$

205 / 370

Oracle de Grover 3/3

Par rebond de phase, on a implémenté l'oracle qui réalise l'action suivante sur les qubits d'input :

- $|x\rangle$ est inchangé si $f(x) = 0$
- $|x\rangle$ est transformé en son opposé $|x\rangle$ si $f(x) = 1$

Cet opérateur est crucial dans l'implémentation de l'algorithme de Grover

Opérateur de diffusion de Grover 1/2

Considérons l'opérateur D défini par

$$D = 2\left|0\right\rangle\left\langle 0\right| - I$$

Cet opérateur correspond à la matrice diagonale suivante

$$D = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & & \\ 0 & 0 & -1 & & \\ \vdots & & & \ddots & \\ 0 & & & & -1 \end{pmatrix}$$

Il est clair que cette matrice est à la fois unitaire et hermitienne. C'est un opérateur quantique valide.

Opérateur de diffusion de Grover 2/2

Considérons à présent l'opérateur G défini par

$$G = H^{\otimes n}.D.H^{\otimes n} = H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right| - I)H^{\otimes n}$$

On a, compte tenu du fait que $H = H^{\dagger}$

$$\begin{aligned} G &= H^{\otimes n}(2\left|0\right\rangle\left\langle 0\right| - I)H^{\otimes n} \\ &= 2H\left|0\right\rangle\left\langle 0\right| H^{\dagger} - HIH \\ &= 2\left|+\right\rangle\left\langle +\right| - I \\ &= \frac{2}{2^n}\sum_i \left|i\right\rangle \sum_j \left\langle j\right| - I \\ &= \frac{2}{2^n}\sum_{i,j} \left|i\right\rangle\left\langle j\right| - I \end{aligned}$$

Effet de l'opérateur de diffusion 1/2

Observons l'effet de l'opérateur G sur un état $|\phi\rangle = \sum_k c_k |k\rangle$

$$
\begin{aligned}
G|\phi\rangle &= (\frac{2}{2^n}\sum_{i,j}|i\rangle\langle j| - I)\sum_k c_k|k\rangle \\
&= \frac{2}{2^n}\sum_{i,j,k} c_k|i\rangle\langle j|k\rangle - \sum_k c_k|k\rangle \\
&= \frac{2}{2^n}\sum_{i,j,k} c_k\delta_{jk}|i\rangle - \sum_k c_k|k\rangle \\
&= \frac{2}{2^n}\sum_{i,k} c_k|i\rangle - \sum_k c_k|k\rangle \\
&= \frac{2}{2^n}\sum_k c_k\sum_i|i\rangle - \sum_k c_k|k\rangle \\
&= 2.\frac{\sum_k c_k}{2^n}\sum_i|i\rangle - \sum_k c_k|k\rangle
\end{aligned}
$$

Effet de l'opérateur de diffusion 2/2

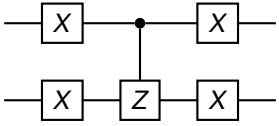
On remarque que le premier terme est la moyenne des coefficient c_k qui sont au nombre de 2^n, on note $< c >$ cette moyenne. On peut dès lors écrire

$$G|\phi\rangle = 2. < c > \sum_i |i\rangle - \sum_k c_k |k\rangle$$
$$= \sum_k (2 < c > -c_k) |k\rangle$$

Cet opérateur réalise l'effet "miroir par rapport à la moyenne" pour chaque coefficient c_k. On le nomme opérateur de diffusion de Grover.

Opérateur de diffusion sur 2 qubits sous la forme d'un circuit

Considérons le circuit suivant à 2 qubits :



Si l'on cherche à écrire la matrice 4×4 qui lui correspond, il s'agit du produit $(X \otimes X) \times CZ \times (X \otimes X)$.

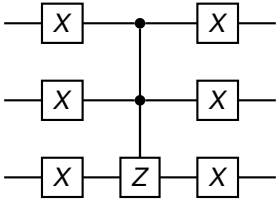
Calcul sur 2 qubits

$$
\begin{aligned}
(X \otimes X) \times CZ \times (X \otimes X) &= \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= -\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\
&= -(2\,|0\rangle\langle 0| - I) \equiv 2\,|0\rangle\langle 0| - I
\end{aligned}
$$

Ce circuit produit l'effet de la matrice D du début, module un produit par -1. Mais, la mesure ne prend en compte que le module et perd les informations de phase, ce circuit est totalement équivalent à la matrice D .

Circuit de l'opérateur de diffusion sur 3 qubits

Avec trois quabits, réalisera le produit suivant



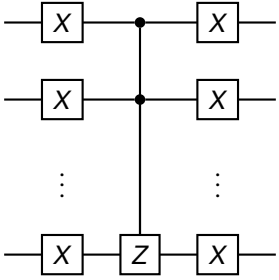
Le calcul matriciel, c'est la force

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

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Grover sur n qubits

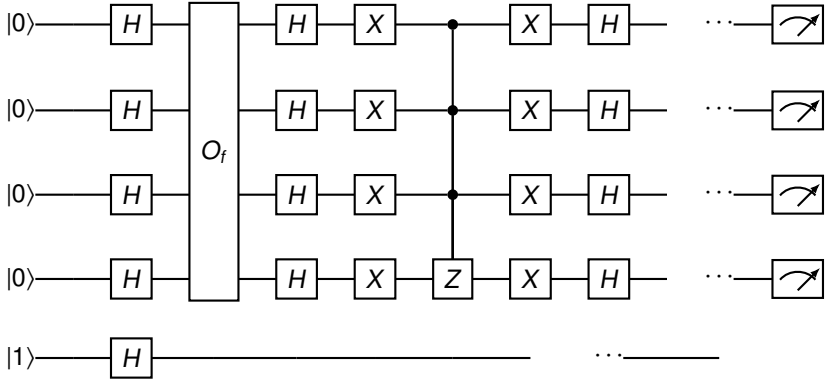
Par récurrence, on peut démontrer que



Produit un opérateur équivalent à la matrice $-D$ sur n qubits.

Circuit (simple) de l'algorithme de Grover sur 4 qubits

On considère le circuit suivant



On voit : l'oracle "spécial", suivi de l'opérateur de diffusion encadré par des *H* puis des mesures.

Un peu de calcul...

Soit k_0 l'indice pour lequel la fonction f n'est pas nulle, on peut écrire la superposition uniforme ainsi (en notant $N = 2^n$ pour alléger la notation).

$$\begin{aligned}
|\Phi_0\rangle = \frac{1}{\sqrt{N}} \sum_j |j\rangle &= \frac{1}{\sqrt{N}} \sum_{j \neq k_0} |j\rangle + \frac{1}{\sqrt{N}} |k_0\rangle \\
&= \frac{\sqrt{N-1}}{\sqrt{N-1}} \frac{1}{\sqrt{N}} \sum_{j \neq k_0} |j\rangle + \frac{1}{\sqrt{N}} |k_0\rangle \\
&= \frac{\sqrt{N-1}}{\sqrt{N}} \sum_{j \neq k_0} \frac{1}{\sqrt{N-1}} |j\rangle + \frac{1}{\sqrt{N}} |k_0\rangle
\end{aligned}$$

Si on note $|\phi_0\rangle$, le premier terme, qui correspond à une "superposition uniforme partielle", on obtient

$$\text{si } |\phi_0\rangle = \frac{1}{\sqrt{N-1}} \sum_{j \neq k_0} |j\rangle \text{ alors } \frac{1}{\sqrt{N}} \sum_j |j\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |\phi_0\rangle + \frac{1}{\sqrt{N}} |k_0\rangle$$

Introduction d'un angle

On remarque que les deux coefficients ont le bon goût d'être compris entre 0 et 1 et d'avoir des carrés dont la somme vaut 1, il existe donc un angle θ tel que

$$\theta \in [0, \pi/2], cos(\theta) = \frac{\sqrt{N-1}}{\sqrt{N}}, sin(\theta) = \frac{1}{\sqrt{N}}$$

Par conséquent, la superposition uniforme peut s'écrire, ainsi

$$\frac{1}{\sqrt{N}} \sum_j |j\rangle = cos(\theta) |\phi_0\rangle + sin(\theta) |k_0\rangle$$

Comme N est grand, l'angle θ sera petit, son sinus très proche de 0 et son cosinus très proche de 1.

Diffusion et portes H agissant ensemble

Revenons sur le circuit un peu plus haut, o remarque que le circuit qui définit la diffusion de Grover est encadré par une bordée de portes H avant et après. Cela revient à modifier l'opérateur de diffusion qui devient

$$G = H^{\otimes n} D H^{\otimes n} = 2 |\Phi_0\rangle \langle \Phi_0| - I$$

On notera que, puisque $|k_0\rangle$ est orthogonal à chaque vecteur dans $|\phi_0\rangle$, il a un produit scalaire nul avec $|\phi_0\rangle$.

$$\begin{aligned} G &= 2 |\Phi_0\rangle \langle \Phi_0| - I \\ &= 2(cos(\theta) |\phi_0\rangle + sin(\theta) |k_0\rangle)(cos(\theta) \langle \phi_0| + sin(\theta) \langle k_0|) - I \\ &= 2(cos^2(\theta) |\phi_0\rangle \langle \phi_0| + sin^2(\theta) |k_0\rangle \langle k_0|) + 2cos(\theta)sin(\theta)[|\phi_0\rangle \langle k_0| + |k_0\rangle \langle \phi_0|] \end{aligned}$$

L'opérateur G est une réflexion selon un hyperplan

Par conséquent

$$\begin{aligned} G|k_0\rangle &= 2sin^2(\theta)|k_0\rangle + 2cos(\theta)sin(\theta)|\phi_0\rangle - |k_0\rangle \\ &= (2sin^2(\theta) - 1)|k_0\rangle\, 2cos(\theta)sin(\theta)|\phi_0\rangle \\ &= cos(2\theta)|k_0\rangle - sin(2\theta)|\phi_0\rangle \\ G|\phi_0\rangle &= 2cos^2(\theta)|\phi_0\rangle + 2cos(\theta)sin(\theta)|k_0\rangle - |\phi_0\rangle \\ &= (2cos^2(\theta) - 1)|\phi_0\rangle\, 2cos(\theta)sin(\theta)|k_0\rangle \\ &= sin(2\theta)|k_0\rangle + cos(2\theta)|k_0\rangle \end{aligned}$$

Nous allons démontrer que, après m itérations de l'opérateur de diffusion de Grover, on trouve l'état $|\Phi_m\rangle$ défini par

$$\begin{aligned} G^m|k_0\rangle &= cos((2m-1)\theta)|k_0\rangle - sin((2m+1)\theta)|\phi_0\rangle \\ G^m|\phi_0\rangle &= sin((2m-1)\theta)|k_0\rangle + cos((2m+1)\theta)|\phi_0\rangle \end{aligned}$$

Démonstration par récurrence 1/2

L'état initial, qui correspond à $m = 0$ est la superposition uniforme qui s'écrit, comme on vient de le voir, sous la forme

$$cos(\theta)\,|\phi_0\rangle + sin(\theta)\,|k_0\rangle$$

ce qui forme le cas initial $m = 0$ Supposons que la propriété est vraie au rang m, démontrons là au rang $m + 1$

$$\begin{aligned}
G^{m+1}\,|k_0\rangle &= G.G^m\,|k_0\rangle = G(cos((2m-1)\theta)\,|k_0\rangle - sin((2m-1)\theta)\,|\phi_0\rangle) \\
&= cos((2m-1)\theta)[cos((2\theta)\,|k_0\rangle - sin(2\theta)\,|\phi_0\rangle] \\
&- sin((2m-1)\theta)[sin(2\theta\,|k_0\rangle + cos(2\theta)\,|\phi_0\rangle] \\
&= cos((2m-1)\theta)cos((2\theta)\,|k_0\rangle - cos((2m-1)\theta)sin(2\theta)\,|\phi_0\rangle \\
&- sin((2m-1)\theta)sin(2\theta\,|k_0\rangle - sin((2m-1)\theta)cos(2\theta)\,|\phi_0\rangle \\
&= [cos((2m-1)\theta)cos((2\theta) - sin((2m-1)\theta)sin(2\theta)]\,|k_0\rangle \\
&- [cos((2m-1)\theta)sin(2\theta) + sin((2m-1)\theta)cos(2\theta)]\,|\phi_0\rangle \\
&= cos((2m+1)\theta)\,|k_0\rangle - sin((2m+1)\theta)\,|\phi_0\rangle
\end{aligned}$$

Démonstration par récurrence 2/2

$$
\begin{aligned}
G^{m+1}|\phi_0\rangle &= G.G^m|\phi_0\rangle = G(sin((2m+1)\theta)|k_0\rangle + cos((2m+1)\theta)|\phi_0\rangle) \\
&= sin((2m-1)\theta)[cos(2\theta)|k_0\rangle - sin(2\theta)|\phi_0\rangle] \\
&+ cos((2m-1)\theta)[sin(2\theta)|k_0\rangle + cos(2\theta)|\phi_0\rangle] \\
&= sin((2m-1)\theta)cos(2\theta)|k_0\rangle - sin((2m-1)\theta)sin(2\theta)|\phi_0\rangle \\
&+ cos((2m-1)\theta)sin(2\theta)|k_0\rangle + cos((2m-1)\theta)cos(2\theta)|\phi_0\rangle \quad de \\
&= [sin((2m-1)\theta)cos(2\theta) + cos((2m-1)\theta)sin(2\theta)]|k_0\rangle \\
&+ [cos((2m-1)\theta)cos(2\theta) - sin((2m-1)\theta)sin(2\theta)]|\phi_0\rangle \\
&= sin((2m+1)\theta)|k_0\rangle + cos((2m+1)\theta)|\phi_0\rangle
\end{aligned}
$$

ce qui valide la propriété au rang suivant

Itération multiples de l'opérateur de Grover

Plus on exécute l'algorithme plus m augmente, plus le $cos((2m+1)\theta)$ augmente plus il devient probable de mesurer $|k_0\rangle$, mais il ne faut pas aller trop loin (sinon on déépasse 1 et on commence à perdre des chances de voir l'état voulu).

Si on veut observer $|k_0\rangle$ avec une probabilité élevée, il faut maximiser le sinus, donc il faut que l'angle soit aussi proche que possible de $\pi/2$, soit

$$2(m-1)\theta) \approx \pi/2$$

et donc

$$m \approx \frac{\pi}{4\theta}$$

Mais par définition, on a

$$sin(\theta) = \sqrt{\frac{1}{2^n}}$$

Estimation de la valeur de m

Si n est assez grand, θ est très petit et $sin(\theta) \approx \theta$ au premier ordre. Si l'on considère que l'inverse de θ est très grand face à $1/2$, on peut écrire

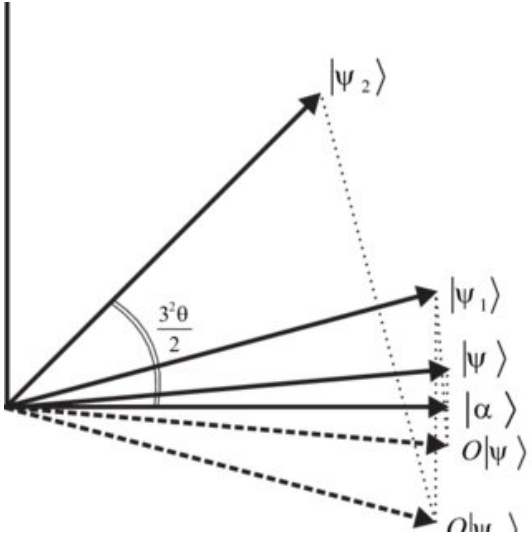
$$m \approx \frac{\pi}{4\theta} \text{ soit } m \approx \frac{\pi}{4}\sqrt{2^n}$$

On prendra donc pour m la valeur entière la plus proche de $\frac{\pi}{4}\sqrt{2^n}$

$$m = \lfloor \frac{\pi}{4\theta} \text{ soit } m \approx \frac{\pi}{4}\sqrt{2^n} \rfloor$$

On rappelle qu'on connaît θ puisque $\frac{\sqrt{N-1}}{\sqrt{N}}$, on peut donc construire tout de suite le circuit qui donne la mesure optimale.

Vision géométrique



Cas général : la fonction n'est pas nulle sur plusieurs points

On a supposé que f était nulle partout sauf en un point ? Que se passe-t-il si cette fonction est non-nulle sur k valeurs ?

L'approche est globalement la même, l'angle θ sera défini par

$$sin(\theta) = \sqrt{\frac{k}{N}}$$

et

$$|\phi_0\rangle = \sum_{x,f(x)=0} \sqrt{\frac{1}{N-k}} |x\rangle$$

Si on fait l'hypothèse alors le sinus peut se simplifier au premier ordre.

$$m = \lfloor \frac{\pi}{4} \sqrt{\frac{2^n}{k}} \rfloor$$

Trouver le m optimal est difficile car k est généralement inconnu.

Utilisation de Grover 1/2

L'algorithme de Grover est traditionnellement exploité dans le cadre de l'exploitation des bases de données. Supposons que l'on veuille trouver le sous-ensemble E' d'un ensemble E, défini par la conformité à un certain critère connu. Il suffit de construire une fonction f qui soit non nulle sur E' et nulle en dehors.

Là ou un algorithme classique a des performances en $O(N)$ si N est le cardinal de E, l'algorithme de Grover aura des performances en $O(\sqrt{N})$, un gain quadratique significatif (une recherche qui prendrait une journée, soit 86400 secondes, se ferait en 293 secondes via l'algorithme de Grover, soit moins de 5 minutes).

Utilisation de Grover 2/2

Des applications de Grover peuvent se trouver en cryptographie, car on peut ramener certains problèmes à la définition en compréhension d'un sous-ensemble (donc à construire la fonction f évoquée plus haut). La cryptographie se ramène souvent à calculer une valeur de hachage, qui est utilisée pour le chiffrement, calculée à partir d'un mot de passe qui reste secret (ce mot de passe peut toujours se ramener à une chaina binaire grâce au code ASCII). Il suffit de construire la fonction qui, pour une chaine donnée, compare son image par la fonction de hachage à la valeur cible pour bâtir f

D'une manière assez générique, Grover s'applique à tous les problèmes qui peuvent se ramener à la recherche d'une image réciproque : connaissant une fonction F, connaissant une valeur y_0, quel est l'ensemble E tel que $\forall x \in E, F(x) = y_0$.

Critiques sur l'algorithme de Grover

L'algorithme de Grover est parfois controversé et critiqué. On peut résumer ces critiques sous la forme "Grover permet de trouver des choses que l'on connaît déjà", le fait de pouvoir construire un oracle est souvent associé avec l'idée que le problème est déjà résolu. D'autres objections soulignent que dans les cas les plus intéressants, il ne sera probablement pas possible de construire de construire un oracle, capable de calculer sur un état superposé. Le cas le plus classique, qui applique Grover à la recherche dans une base de donnée, se heurte au fait que cette implémentation est impossible, à moins de disposer d'une "mémoire quantique" de grande taille. Au jour où ce document est rédigé, on sait expérimentalement implémenter une mémoire quantique d'un unique qubit.

Par ailleurs, Grover suppose qu'il est possible d'intriquer un grand nombre de qubits ensemble, ce qui est une limitation très forte au regard des implémentations physiques des qubits.

Plan

23 Les concepts de bases

24 Correction des erreurs

25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

Introduction à la cryptographique quantique

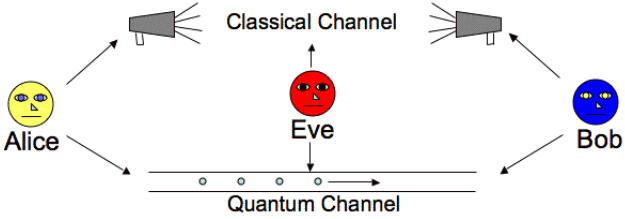
La cryptographie quantique exploite les principes de la mécanique quantique et de l'informatique quantique pour gérer des mécanismes de chiffrement.

En général, à l'état actuel des technologies, ces mécanismes vont majoritairement exploiter des "qubits volants", souvent implémentés par des photons. L'état des qubits sera implémenté par l'angle de polarisation des photons.

Problématique

On est ici sur une logique de construction de clefs binaires entre deux parties, en s'appuyant sur des mécanismes quantiques. .

Cette clef binaire pourra être utilisé pour chiffrer le message avec un simple XOR ou bien être impliquée dans un mécanisme de chiffrement plus complexe.

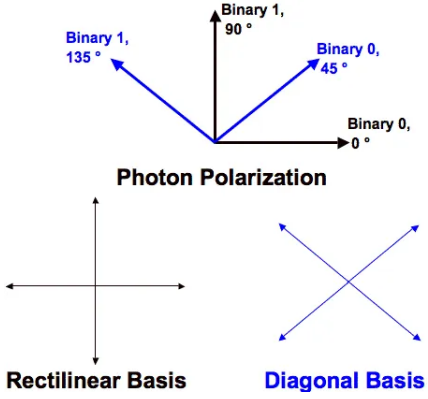


Dans ce schéma, Alice et Bob dispose d'un canal de communication quantique, et d'un canal publique, non sécurisé (par ondes radio, ou par email). Eve, l'attaquant, peut facilement voir ce canal.

Le protocole BB84 1/2

Le premier protocole de chiffrement quantique a été conçu en 1984 par Charles Benett et Gilles Brassard.

Il s'appuie sur des qubits implémentés via des photons polarisés. Ces derniers peuvent être polarisés de deux manières différentes, une polarisation rectiligne et une polarisation diagonale



233 / 370

Le protocole BB84 2/2

Du point de vue du formalisme, on utilisera des qubits individuels exprimés soit dans la base canonique $(|0\rangle, |1\rangle)$, soit dans la base de Bell $(|+\rangle, |-\rangle)$.
Le fonctionnement est le suivant :

1. Alice choisit de manière aléatoire une chaine de bits ;
2. pour chaque bit, Alice choisit une base et envoie un photon encodé selon cette base, par exemple, si elle voit le bit 0 et la base $(|+\rangle, |-\rangle)$, elle expédie $|+\rangle$ et si elle voit 1 et la base $(|0\rangle, |1\rangle)$, elle envoie $|1\rangle$;
3. Bob reçoit les photons, mais sans savoir dans quelle base ils doivent être interprétés, il choisit alors une base de manière aléatoire parmi les deux disponibles et effectue une mesure ;
4. Alice et Bob communiquent alors sur le canal classique, Bob va publier la liste des bases qu'il a utilisées pour chaque photon, et Alice lui indique quels photons il a correctement interprétés ;
5. Alice et Bob supprime les photons sur lesquels ils n'ont pas des bases identiques. Ils disposent alors d'une chaine de bits identique de chaque côté qu'ils peuvent utiliser pour chiffer un message .

Exemple de BB84

Voyons un exemple d'échange dans le tableau suivant :

Bits / Alice	0	1	1	0	1	0	0	1
Bases / Alice	01	01	+-	01	+-	+-	+-	01
Photons émis	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bases / Bob	01	+-	+-	+-	01	+-	01	01
Mesures / Bob	$\|0\rangle$	$\|+\rangle$ / $\|-\rangle$	$\|-\rangle$	$\|+\rangle$ / $\|-\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|+\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|1\rangle$
Clef	0		1			0		1

235 / 370

Attaque MIM sur BB84

Le protocole BB84 peut souffrir d'une attaque classique de type *Man In the Middle*. Eve s'interpose entre Alice et Bob,choisit une base au hasard et tente de faire une mesure.

On peut imaginer que Eve vient intercaler un filtre polariseur entre Alice et Bob. Les photons émis par Alice arriveront jusqu'à Bob, mais ils seront changés par la lecture effectuée par Eve.

Bits/A	0	1	1	0	1	0	0	1
Bases/A	01	01	+-	01	+-	+-	+-	01
Photons	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bases/E	+-	01	+-	01	+-	01	01	01
Après E	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|1\rangle$
Bases / B	01	+-	+-	+-	01	+-	01	01
Mesures/B	$\|0\rangle$ / $\|1\rangle$	$\|+\rangle$ / $\|-\rangle$	$\|-\rangle$	$\|+\rangle$ / $\|-\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|+\rangle$ / $\|-\rangle$	$\|0\rangle$ / $\|1\rangle$	$\|1\rangle$
Clef E	0		1			0		1
Clef B	0 / 1		**1**			0 / 1		**1**

La clef correcte est 0101 mais du fait de la présence d'Eve, Bob peut voir une clef erronée comme 1101 ou 1111. Seuls les bits où Alice, Eve et Bob ont choisi les mêmes bases ne seront pas corrompus, les autres sont potentiellement faussés.

Protection de BB84 contre une attaque MIM

Alice et Bob peuvent se protéger d'une attaque MIM en choisissant de sacrifier une partie de la clef négociée.

Par exemple, ils peuvent choisir de se communiquer sur le canal classique une moitié des clefs qu'ils ont bâties. S'ils observent des valeurs différentes, ils savent qu'il y a une corruption sur le canal quantique et jettent la clef produite.

Dans notre exemple, Alice et Bob choisissent de sacrifier 2 bits sur 4, Alice expose 01 et Bob expose 11 à cause d'Eve. Ils savent qu'il y a un problème et recommencent le processus.

Pour chaque bit où Alice et Bob ont choisit les mêmes bases, il y a 1 chance sur 4 pour Eve de passer inaperçu. Si n bits sont sacrifiés pour détecter une attaque MIM, la probabilité qu'Eve ne soit pas détectée est de $\frac{1}{4^n}$ qui tend vers 0 quand n augmente.

Le protocole B92

Le protocole B92 est une évolution de BB84 proposée par Charles Benett, co-auteur de BB84, en 1992. Il est moins sensible au bruit sur le canal quantique.
On dispose de deux bases, $(|0\rangle, |1\rangle)$ et $(|+\rangle, |-\rangle)$, mais on n'utilisera qu'un seul vecteur de chaque base. On encodera par exemple le bit 0 toujours via le qubit $|0\rangle$ et le bit 1 via $|+\rangle$.

Le protocole est le suivant :

1. pour chaque bit, Alice envoie un photon $|0\rangle$ ou $|+\rangle$ selon la valeur du bit ;
2. pour chaque photon, Bob choisit une base aléatoirement, mais il oriente son détecteur perpendiculaire aux valeurs qu'il pense avoir été utilisées par Alice.
   - s'il choisit $(|0\rangle, |1\rangle)$, il cherchera à détecter $|1\rangle$;
   - s'il choisit $(|+\rangle, |-\rangle)$, il cherchera à détecter $|-\rangle$;
3. si Bob s'est trompé de base, il croit avoir détecté un état superposé, et le détecteur va détecter 50% de l'état
4. si Bob a choisi la bonne base, le détecteur ne voit rien.
5. Bob indique à Alice sur quels tirs il a choisi la bonne base, Alice rejette les autres valeurs et les deux connaissentà présent la clef commune.

Le protocole E91

Le protocole E91 a été créé par Artur Ekert en 1991. Ce protocole a été inspiré à son auteur par l'expérience de Alain Aspect en 1982. Il s'appuie sur une paire de photons intriqués.

On rappelle cette propriété de la paire EPR :

$$\frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

En effet

$$|{+}{+}\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle + |01\rangle + |10\rangle)$$

$$|{-}{-}\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle - |01\rangle - |10\rangle)$$

$$\frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle) = \frac{1}{2\sqrt{2}}(2\,|00\rangle + 2\,|11\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Principe de E91

Le protocole E91 est fortement associé avec l'expérience CHSH, laquelle a été concrêtisée par Alain Aspect en 1982.

Dans ce mécanisme, on suppose qu'on dispose d'une source capable de produire une paire EPR de photons intriqués $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, l'un des photons est expédié à Alice, l'autre à Bob. Pour chaque photon, Alice va choisir aléatoirement une base $(|0\rangle, |1\rangle)$ ou $(|+\rangle, |-\rangle)$. Ce faisant, on effondre l'état de la paire intriquée, ce qui change l'état des photons de Bob.

De son côté, Bob va choisir des bases de manière aléatoire et mesurer ses photons effondrés. Il publie ensuite ses bases à Alice, qui lui indique quels choix ont été corrects. Bob et Alice ne conservent que les bons choix pour construire une clef de chiffrement.

Exemple de run de E91

Base A	01	01	+-	01	+-	+-	+-	01
Read A	01 50/50	01 50/50	+- 50/50	01 50/50	+- 50/50	+- 50/50	+- 50/50	01 50/50
Bits A	01 50/50	01 50/50	01 50/50	01 50/50	01 50/50	01 50/50	01 50/50	01 50/50
Base B	01	+-	01	01	+-	01	+-	01
Read B	01 50/50	+- 50/50 +- 50/50	01 50/50 01 50/50	01 50/50	+- 50/50	01 50/50 01 50/50	+- 50/50	01 50/50
Bits B	01 50/50	01 50/50 01 50/50	01 50/50 01 50/50	01 50/50	01 50/50	1 50/50 01 50/50	01 50/50	01 50/50
Read Same	100%	50%/50%	50%/50%	100%	100%	50%/50%	100%	100%
Key	0 ou 1	-	-	0 ou 1	0 ou 1	-	0 ou 1	0 ou 1

241/370

Exposition de E91 à l'attaque MIM

La présence d'une attaque MIM est possible, Eve peut interposer un filtre polariseur sur le canal quantique, elle fera effondrer l'état mais ni Alice ni Bob. Toutefois, Alice et Bob ont moyen de tester si leurs photons sont oui ou non intriqués, via un test de Bell qui repose sur les inégalités de Bell de la physique quantique. Si le test échoue, alors Eve est démasquée et la clef n'est pas utilisable.

Pour compliquer la possibilité de produire une attaque, E91 s'utilise par- fois avec 3 bases, donc 3 types de polarisation différents.

Plan

23 Les concepts de bases

24 Correction des erreurs

25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

Plan

23 Les concepts de bases

24 Correction des erreurs

25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

Plan

23 Les concepts de bases

24 Correction des erreurs

25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

Plan

23 Les concepts de bases

24 Correction des erreurs

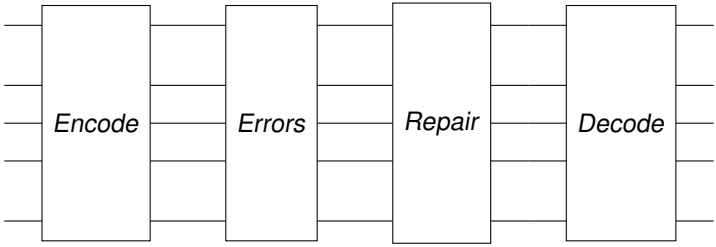
25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

Schéma de corrections des erreurs

On peut modéliser la correction des erreurs de la manière suivante



Qubit logique sur 3 qubits physiques

On va chercher à corriger un bit flip sur des qubits physiques en mappant un qubit physique sur 3 qubits logiques

Dans cet exemple, nous allons représenter un qubit par 3 qubits. On va choisir l'encodage simple suivant

$$|0\rangle \mapsto |000\rangle \text{ et } |1\rangle \mapsto |111\rangle$$

Au final, on choisir la valeur de bit la plus représentée dans la mesure comme valeur du qubit final, ainsi la mesure de $|010\rangle$ sera traduite par la mesure de $|0\rangle$.

Cette manière d'encoder permet de corriger une erreur de *bit flip* sur un seul qubit. Supposons que la probabilité que se produise un *bit flip* sur un seul qubit est de p, la probabilité de ne pas produire une erreur est donc de $1 - p$.

Calcul de probabilités

Si je fais plusieurs opérations, je peux produire une erreur à chaque étape. les probabilités d'erreurs évoluent. Supposons que je fasse 3 opérations, les probabilités d'erreur sont

pas d'erreur du tout	$(1-p)^3$
Un qubit en erreur (3 cas possibles)	$3p(1-p)^2$
Deux qubits en erreur (3 cas possibles)	$3p^2(1-p)$
Trois erreurs	p^3

On sait corriger les deux premiers cas, dont la probabilité conjointe sera

$$\begin{aligned} Proba_{OK} &= (1-p)^3 + 3p(1-p)^2 \\ &= 1 - 3p + 3p^2 - p^3 + 3p(1 - 2p + p^2) \\ &= 1 - 3p + 3p^2 - p^3 v + 3p - 6p^2 + 3p^3 \\ &= 1 - 3p^2 + 2p^3 \end{aligned}$$

249/370

Cas de la double erreur

Les cas à 2 ou 3 erreurs ne sont pas corrigibles, la probabilité que cela se produise est

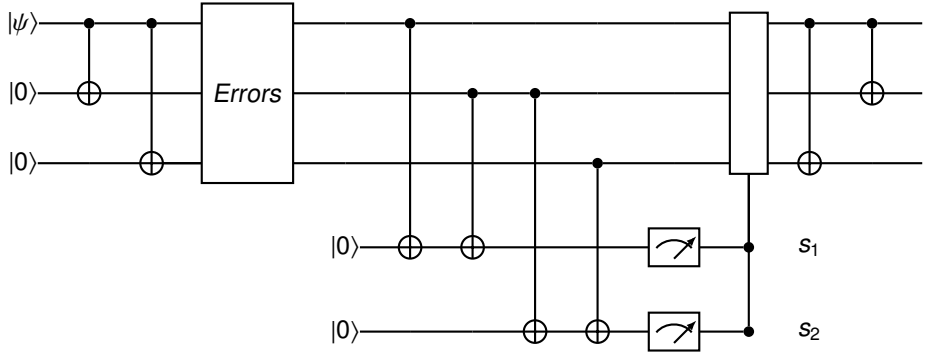
$$\begin{aligned} Proba_{NOK} &= 3p^2(1-p) + p^3 \\ &= 3p^2 - 3p^3 + p^3 \\ &= 3p^2 - 2p^3 \end{aligned}$$

C'est donc la probabilité p^2 qui sera la plus significative, si p est initialement assez petit, la probabilité de retomber dans un cas que l'on sait corriger devient assez important.

En effet, si on suppose qu'un bit flip se produira dans 1 pour cent des cas, on aura une erreur sur 3 opérations avec une probabilité de l'ordre de 1 pour dix mille. Augmenter le nombre de qubits augmente cet effet.

Corriger un bit flip sur 3 qubit

Considérons le circuit suivant. Il compose un encodage / décodage à même de gérer une erreur de type bit flip sur un qubit logique, encodé sur 3 qubits physiques.



Circuit de correction

Si l'état initial est $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, les deux premières portes CNOT vont encoder sur 3 qubits l'état $|\psi_3\rangle = \alpha|000\rangle + \beta|111\rangle$. On plonge un espace de Hilbert à 2 dimensions dans un espace à 8 dimensions.

Il se produit des erreurs "bit flips", sur les qubits, cela revient à ajouter une porte X sur l'un des trois premiers qubits, ou sur aucun. Il y a quatre cas à envisager.

- aucune erreur, cela revient à appliquer $E_0 = I \otimes I \otimes I$
- une erreur sur le premier qubit, on applique $E_1 = X \otimes I \otimes I$
- une erreur sur le second qubit, on applique $E_2 = I \otimes X \otimes I$
- une erreur sur le troisième qubit, on applique $E_3 = I \otimes I \otimes X$

Les quatre opérateurs $\{E_0, E_1, E_2, E_3\}$ sont les opérateurs de Kraus pour ce syndrome d'erreur.

Corriger les différents bits flips

On utilise ensuite 2 qubits ancillaires pour identifier le type d'erreur. L'effet des deux portes CNOT contrôlées par deux qubits distrincts permet de savoir si ces deux qubits sont dans le même état canonique ou non. Ainsi, s_1 permet de savoir si les deux premiers qubits sont identiques et s_2 permet de savoir si les deux derniers sont identiques. Selon le type d'erreur E_k réalisé, on va avoir différentes valeurs de s_1 et s_2

s_1	s_2	Opérateur de Kraus
0	0	$I \otimes I \otimes I$
0	1	$I \otimes I \otimes X$
1	0	$X \otimes I \otimes I$
1	1	$I \otimes X \otimes I$

La valeur du couple (s_1, s_2) permet donc de savoir le type d'opérateur de Kraus appliqué, on est dès lors à même de le corriger. La situation est ici similaire à l'algorithme de téléportation quantique on va appliquer ou non des portes X en fonctions de la mesure afin de corriger l'effet du syndrome d'erreur.

Vision mathématique

Envisageons la situation d'un point de vue mathématique. L'encodage plonge $\mathbb{C}^2$ dans $\mathbb{C}^8$, plus précisément dans l'hyperplan généré par $|000\rangle$ et $|111\rangle$. Les différents opérateurs de Kraus viennent déplacer l'état dans un autre hyperplan

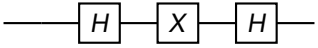
- E_0 nous laisse dans l'hyperplan généré par $|000\rangle$ et $|111\rangle$
- E_1 nous envoie dans l'hyperplan généré par $|100\rangle$ et $|011\rangle$
- E_2 nous envoie dans l'hyperplan généré par $|010\rangle$ et $|101\rangle$
- E_3 nous envoie dans l'hyperplan généré par $|001\rangle$ et $|110\rangle$

Ces 4 hyperplans sont orthogonaux les uns avec les autres. La mesure de s_1 et s_2 permet de caractériser l'hyperplan en question. Il suffit alors d'appliquer l'opérateur X sur le bon qubit pour corriger l'erreur et revenir dans l'hyperplan généré par $|000\rangle$ et $|111\rangle$.

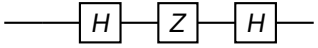
On décode ensuite les 3 qubits pour revenir de $\mathbb{C}^8$ vers $\mathbb{C}^2$ avec les deux dernières portes CNOT.

Corriger un phase flip sur une répétition à trois qubits 1/2

On suppose à présent que les syndromes d'erreur sont constitués de portes Z, des inversions de phase. L'encodage et le circuit précédent est utilisable si l'on se rappelle qu'une porte Z correspond à une porte X encadré par deux portes H

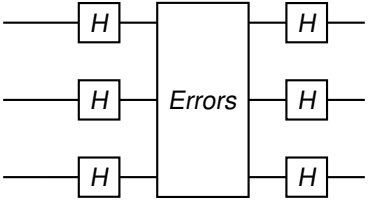


De même, une porte Z est une porte X encadrée par deux portes H



Corriger un phase flip sur une répétition à trois qubits 2/2

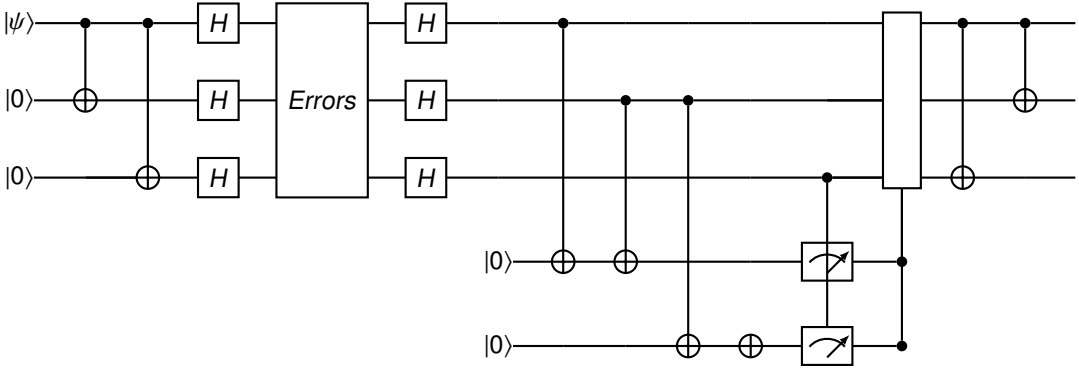
Par conséquent, si on encadre le syndrome d'erreur, qui est constitué de portes Z, avec des portes H, on va soit appliquer deux fois H (et ne rien faire) soit appliquer *HZH* équivalent à X. On peut modifier le circuit précédent en remplaçant le syndrome d'erreur par



256 / 370

Circuit pour corriger les phase flips sur 3 qubits

Le circuit suivant permet donc de corriger les erreurs de phase flips sur un seul des trois qubits.



257/370

Correction des phase flips et des bit flips avec neuf qubits

Plaçons nous dans un exemple encore plus générique où l'on cherche à corriger, sur un seul qubit logique, des erreurs de type X, Y et Z. Pour ce faire, on va utiliser neuf qubits physiques.

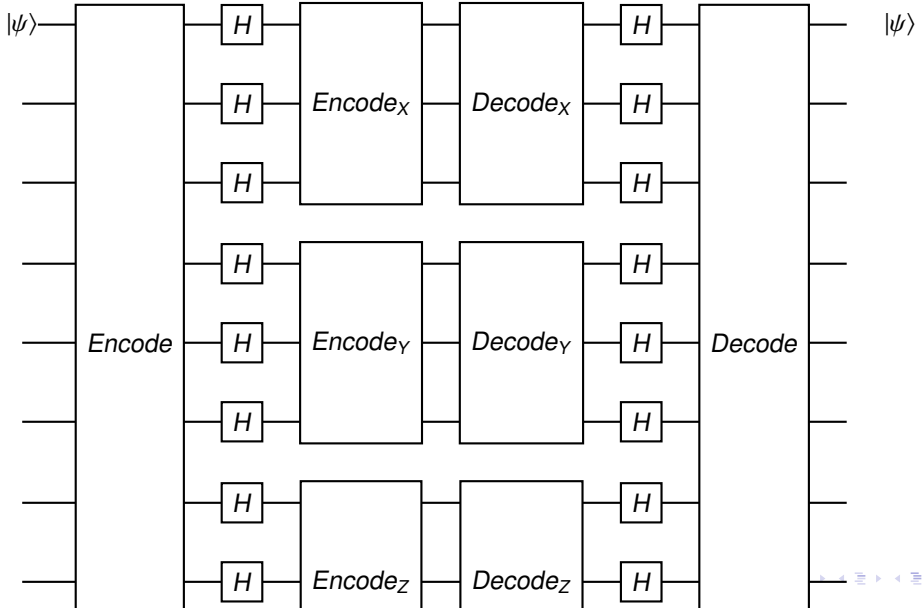
D'un point de vue mathématique, on modélise l'erreur avec la transformation de Stirespring suivant

$$|\psi\rangle|e\rangle \mapsto |\psi\rangle|e_1\rangle + X|\psi\rangle|e_x\rangle + Y|\psi\rangle\left|e_y\right\rangle + Z|\psi\rangle|e_z\rangle$$

en représentation de Kraus, cela revient à prendre en compte les opérateurs $\{I, X, Y, Z\}$. On rappelle que $Y = iXZ$.

Pour corriger à la fois les trois types d'erreurs, on va utiliser 2 couches de corrections sous la forme du circuit décrit à la planche suivante.
On va d'abord plonger $\mathbb{C}^2$ dans $\mathbb{C}^{2^9}$ et on applique les codes correcteurs sur X, Y et Z sur différents hyperplans orthogonaux. On a donc une phase d'encodage et de décodage à deux niveaux.

Correction des phase flips et des bit flips avec neuf qubits



259/370

Plan

28 Un petit détour par la théorie de la complexité

29 Zoologie de Karp des problèmes NPC

30 Éléments de physique et théorème adiabatique

31 Quelques problèmes classiques

32 QUBO et les autres problèmes NPC

33 Machine Pasqal et problème MIS

34 VQE

35 QAOA

36 Inégalités de Bell

37 Le jeu CHSH

Encore des maths

La base de l'informatique quantique analogique est la théorie de la complexité

Dans les grandes lignes :

- certains problèmes "compliqués" peuvent se traduire sous la forme d'une expérience de physique quantique
- on modifie le problème que l'on veut résoudre pour le ramener à cette expérience
- on fait une "expérience instrumentée" dans un QPU analogique
- on en déduit la solution du problème initial

Parmi les implémentations analogiques, on trouve dans le paysage actuel :

- les QPU D-Wave basés sur des boucles supraconductrices
- les QPU Pasqal basés sur des atomes froids manipulés par des lasers
- les machines quantiques photoniques comme ce que propose Qandela

P et NP

En théorie de la complexité informatique, on identifie différentes classes, parmi elles

- les problèmes **de classe P** peuvent être résolu dans un temps qui varie de manière polynomiale avec la taille du problème. Les problèmes P peuvent être résolus avec du HPC
- les problèmes **de classe NP** sont *non-deterministic polynomial*, le temps de résolution est "pire" que polynomiale, mais si on me propose une solution, vérifier qu'elle résoud effectivement le problème prend un temps polynomial.

ATTENTION : NP ne **signifie pas** non-polynomial (c'est un très mauvais acronyme).

Exemples de P et de NP

Les problèmes polynomiales sont ceux du HPC classique, par exemple

- trouver le PGCD ou le PPCM de deux nombres très grands,
- inverser une matrice,
- savoir si un nombre est premier (algorithme AKS)

Exemple de problème NP : factorisation d'un produit de deux nombres premiers

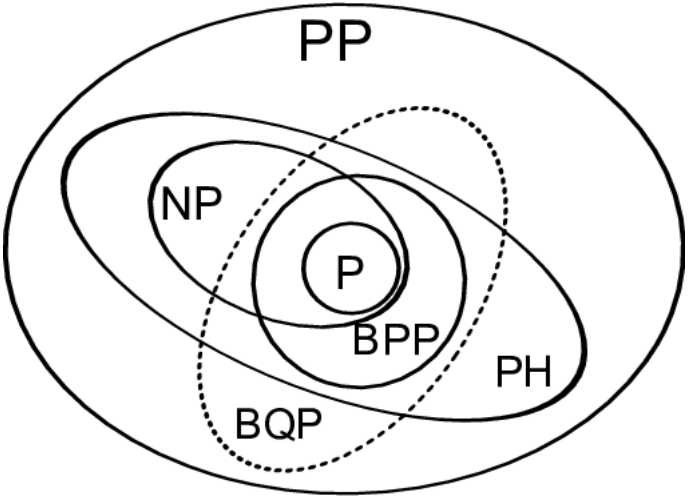
- Soit le nombre 62062883, quelles sont (de tête) ses facteurs ?
- C'est compliqué à trouver...

J'affirme que $62062883 = 7877 \times 7879$,

- On m'a exposé une solution potentielle
- vérifier qu'elle est correcte est simple... on fait la multiplication (c'est polynomial)

La factorisation est typiquement un problème NP.

N et NP ne sont pas les seules classes de complexité



Les problèmes NP-Complets - théorème de Cook

Certains problèmes sont dit **NP-difficiles** si tous les problèmes NP peuvent se ramener à résoudre ce problème en particulier.

Un problème NP qui est également NP-difficile est dit **NP-complet**.

Le théorème de Cook démontre l'existence de problèmes NP-Complets.

Résoudre un problème NP-Complets permet d'y ramener tous les autres problèmes NP au prix d'un algorithme polynomiale.
Il existe de nombreux problèmes NP-complets (QUBO, Voyageur de commerce, SAT, MIS, ...) on en recensait plus de 21 en 1972.

265/370

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Les problèmes de Karp 1/2

En 1972, dans la foulée du théorème de Cook en 1971, le mathématicien Karp recensce 21 problèmes qui sont tous de nature **NPC**, on peut passer de l'un à l'autre au prix d'une transformation polynomiale.

- SATISFIABILITY : le problème SAT pour les formules en forme normale conjonctive
- CLIQUE : le problème de détection de clique dans un graphe
- SET PACKING : Set packing (empaquetage d'ensemble)
- VERTEX COVER : le problème de couverture par sommets, le problème MIS qui lui ets dual
- SET COVERING : le problème de couverture par ensembles
- FEEDBACK ARC SET : feedback arc set
- FEEDBACK NODE SET : feedback vertex set
- DIRECTED HAMILTONIAN CIRCUIT
- UNDIRECTED HAMILTONIAN CIRCUIT
- INTEGER PROGRAMMING : voir optimisation linéaire en nombres entiers
- 3-SAT : problème SAT dont les clauses ont 3 arguments au plus
- CHROMATIC NUMBER : coloration de graphe

267 / 370

Les problèmes de Karp 2/2

- CLIQUE COVER : partition en cliques
- EXACT COVER : couverture exacte
- MATCHING à 3 dimensions : appariement à 3 dimensions
- STEINER TREE : arbre de Steiner
- HITTING SET : ensemble intersectant
- KNAPSACK : problème du sac à dos
- JOB SEQUENCING : séquençage de tâches
- PARTITION : problème de partition
- MAX-CUT : problème de la coupe maximum

268/370

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

L'équation de Schrödinger : les racines du mal...

Pour comprendre l'informatique analogique quantique, il faut garder en tête la notion d'hamiltonien qui dérive directement de l'équation de Schrödinger

$$i\hbar\frac{\partial}{\partial t}\Psi(r,t) = -\frac{\hbar^2}{2m}\nabla^2\Psi(r,t) + V(r,t)\Psi(r,t).$$

La signification des termes est la suivante :

- $\hbar = \frac{h}{2\pi} = 1.05457.10^{-34}$, ou h est la constante de Planck dont la valeur est $6,62607015.10^{-34} m^2 kg/s$
- ∇^2 est le laplacien, aussi défini par $\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$
- m est la masse de la particule ;
- $V(r,t)$ est l'énergie potentielle de la particule à la position r et à l'instant t ;

Hamiltoniens et équation stationnaire

Si l'on s'intéresse aux solutions *stationnaire* de l'équation de Schrödinger, donc indépendante du temps, on peut réduire celle-ci à la forme suivante

$$-\frac{\hbar^2}{2m}\nabla^2 + V(r)]\Psi(r) = E\Psi(r)$$

dans laquelle E est l'énergie de la particule. On désigne l'opérateur $-\frac{\hbar^2}{2m}\nabla^2 + V(r)$, sous le nom d'hamiltonien, noté H.
L'équation de Schrödinger stationnaire se ramène alors à la forme assez simple suivante :

$$H\Psi = E\Psi$$

D'un point de vue formel, résoudre cette équation revient mathématiquement à identifier les valeurs propres et les vecteurs propres de l'hamiltonien H.

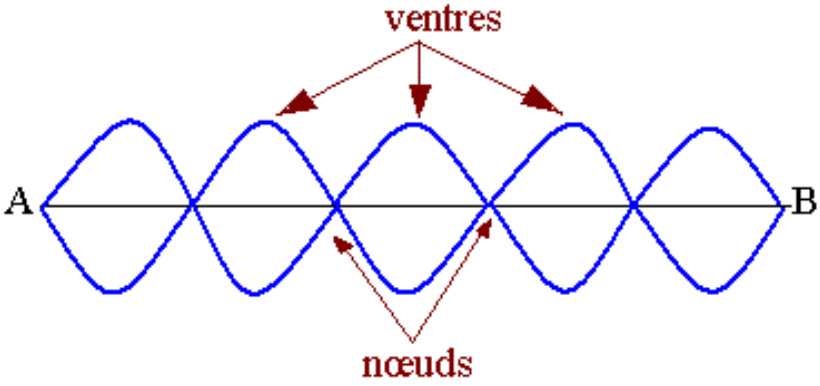
Ondes Stationnaires 1/2

Une onde stationnaire est une onde dont la forme ne dépend pas de l'espace, juste du temps. Par exemple, les harmoniques d'une corde de guitare, et dont les "nœuds" et les "ventres" sont fixes, forme une onde stationnaire. Du point de vue mathématique, on peut écrire que l'onde est le produit de deux facteurs, un qui dépend du temps et un autre qui dépend de l'espace. La fonction d'onde devient donc

$$\Phi(r,t) = \Psi(t)u(r)$$

La fonction $u(r)$ donne la forme en fonction de la position, soit l'amplitude de l'onde au point r, elle est en particulier nulle sur les nœuds de l'onde et maximale sur les ventres. C'est une fonction à valeurs dans $\mathbb{R}$ tandis que $\Phi(t)$ est à valeurs dans $\mathbb{C}$.

Ondes Stationnaires 2/2



Injection dans l'équation de Schrödinger

Si j'injecte le formalisme de l'onde stationnaire $\left|\Phi(r,t)\right\rangle = \left|\Psi(t)\right\rangle u(r)$ cette équation devient

$$i\hbar\frac{\partial}{\partial t}\left|\Psi(t)\right\rangle u(r) = -\frac{\hbar^2}{2m}\nabla^2\left|\Psi(t)\right\rangle u(r) + V(x,t)\left|\Psi(t)\right\rangle u(r).$$

Si j'introduis l'opérateur hamiltonien et que je simplifie les termes qui dépendent de l'espace pour ne garder que ceux qui dépendent du temps, on obtient

$$i\hbar\frac{\partial}{\partial t}\left|\Psi(t)\right\rangle = H\left|\Psi(t)\right\rangle.$$

Solutions stationnaires

Cette équation est à valeur dans $\mathbb{C}^2$, elle est toutefois analogue aux équations dans $\mathbb{R}$. En effet, si l'on considère l'équation suivante

$$\frac{df}{dt} = \alpha f(t)$$

Il est connu que la solution est de la forme

$$f(t) = C.e^{\alpha T} + D$$

L'équation de Schrödinger a la forme suivante, compte tenu de $\hbar = h/2\pi$,

$$\frac{d\left|\Psi(t)\right\rangle}{dt} = -i\frac{2\pi}{h}H\left|\Psi(t)\right\rangle$$

Dont la solution est de la forme

$$\left|\Psi(t)\right\rangle = e^{-\frac{2\pi}{h}H.t}\left|\Psi(0)\right\rangle$$

Opérateurs hermitiens et unitaires

L'opérateur H étant hermitien, iH est antihermitien et l'opérateur $U(t) = e^{-\frac{2\pi}{h}H.t}$ est unitaire. Ce point explique en particulier pourquoi l'informatique quantique ne s'intéresse qu'aux opérateurs unitaires.
Il est intéressant de s'intéresser aux valeurs propres et aux vecteurs propres de l'hamiltonien, soit les vecteurs $|\phi_n\rangle$ et les coefficients réels, homogènes à une énergie, E_n tels que

$$H|\phi_n\rangle = E_n|\phi_n\rangle$$

. En effet, Schrödinger est linéaire, donc les combinaisons linéaires de solutions sont des solutions. Si l'on s'intéresse aux valeurs propres et aux vecteurs propres, l'équation prend la forme

$$\frac{d\left|\phi_n(t)\right\rangle}{dt} = -i\frac{2\pi}{h}E\left|\phi_n(t)\right\rangle$$

Dont la solution est de la forme

$$\left|\phi_n(t)\right\rangle = e^{-\frac{2\pi}{h}E_n.t}\left|\phi_n(0)\right\rangle$$

Connaissant les vecteurs propres de H , les solutions sont

$$\left|\psi(t)\right\rangle = \sum_{i=1}^{n} e^{-\frac{2\pi}{h}E_i.t}\left|\phi_i(0)\right\rangle$$

Thérorème adiabatique

En 1928, les physiciens Max Born et Vladimir Fock, énonce le théorème adiabatique :

> *Un système physique est maintenu dans son état propre instantané si une perturbation donnée agit sur lui suffisamment lentement et s'il y a un intervalle significatif entre la valeur propre et le reste du spectre de l'hamiltonien.*

En d'autres termes, si l'on sait placer un système quantique dans un état d'énergie de base connu, et qu'on le fait évoluer assez lentement et sans lui apporter d'énergie (c'est une évolution adiabatique) alors le système final, qui sera décrit par un nouvel hamiltonien, sera, lui aussi, dans un état d'énergie de base.

Calcul quantique adiabatique

Toute l'informatique quantique analogique s'appuie sur ce principe :

- on encode le problème à résoudre sous la forme d'un hamiltonien ;
- on part d'un système quantique dans un état de base connu avec un hamiltonien de référence connu ;
- on fait évoluer cet hamiltonien depuis celui de référence vers celui qui encode le problème, en respectant les contraintes du théorème adiabatique ;
- on dispose à la fin de l'état de base de l'hamiltonien de destination, celui qui encode le problème

Cette approche est très efficace, elle permet de trouver rapidement et de façon purement analogique, des minima de fonctions très complexes, dont la recherche avec des ordinateurs classiques relèvent de la nature *NP hard*.

Simulated Annealing

Le QUBO peut être résolu, par des méthodes HPC classiques, à l'aide de l'algorithme de *Simulated Annealing* ou "recuit simulé" créé en 1983.

Cet algorithme se base sur une idée empruntée à la métallurgie. Dans ce domaine, il est utile d'amener le métal à son niveau d'énergie le plus bas, où il devient ductile et est plus facile à travailler. Les forgerons réalisent cela en alternant des cycles comprenant des refroidissements lents et des étapes de réchauffage, ou *recuits*[1].

L'algorithme de recuit simulé suit une approche dite "métaheuriistique" qui dérive de l'algorithme de Metropolis-Hastings , issu de la modélisation des phénomènes thermodynamiques. De nombreuses implémentations existent, en particulier dans l'outil Mathematica. Il a souvent été utilisé pour résoudre des problèmes de graphes, en particulier ceux relatifs à la topologie de grands1réseaux informatiques.

1. par opposition, un refroidissement rapide, ou *trempe* va laisser le métat dans un état d'énergie élevé où il est dur mais peut casser, pour forger des couteaux par exemple

Quantum Annealing

Le *Quantum Anneling* est une implémentation matérielle, via des phénomènes quantiques, du QUBO.
La forme quadratique à résoudre est construite sous la forme d'un hamiltonien que l'on peut physiquement construire. On va chercher l'état de base de cet hamiltonien qui correspondra à la valeur minimale, au sens de QUBO, de la forme quadratique.

Dans cette approche adiabatique, on dispose d'un hamiltonien "simple" dont on connaît bien l'état de base, noté H_B et d'un hamiltonien H_P qui représente notre problème (un hamiltonien dont on cherche la plus petite valeur propre). On fait évoluer l'hamiltonien sur le temps T de la manière suivante

$$H(t) = (1 - s(t))H_B + s(t)H_P, s(t = 0) = 0, s(t = T) = 1$$

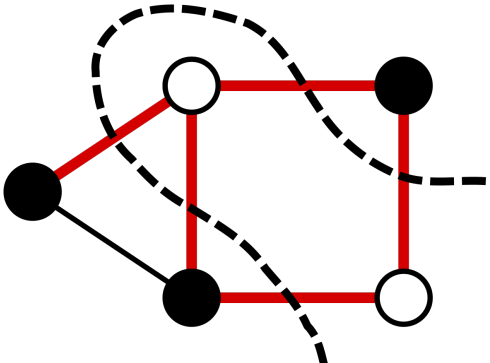
La fonction s est continue, monotone croissante.

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Le problème Max-Cut 1/2

Étant donné un graphe, formé de sommets reliés par des arêtes, il s'agit de réaliser une coupe, donc de séparer le graphe en deux sous-ensembles complémentaires, tels que cette coupe au moins autant d'arêtes que n'importe quelle autre coupe possible.
Le problème Max-Cut est souvent associé à une notion de pondération des arêtes entre les sommets. On peut ainsi définir un "poids de la coupe" qui correspondra à la somme des poids des arêtes coupées. On dira qu'une arête est coupé quand les deux sommets, à chacune de ses extrémités, ne sont pas dans le même ensemble réalisé par la coupe.



Le problème Max-Cut 2/2

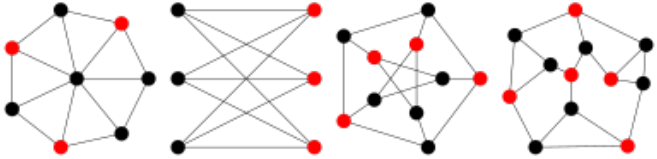
Remarque : d'una manière analogue, on peut définir un Min-Cut, une coupe mininum telle que le poids soit la plus faible valeur possible.
On peut associer deux types de problème à une coupe maximum :

- problème de *décision* : étant donné un graphe G et un entier k, existe-t'il une coupe de G dont le poids est au moins égal à k ;
- problème d'*optimisation* : étant donné un graphe G, quelle est la coupe maximum, celle qui maximise le poids ;

On peut démontrer que le problème Max-Cut se résout en un temps polynomial quand le graphe est planaire, il se ramène alors à l'identification des arêtes du graphe qui n'ont pas de sommets en commun. Un graphe est planaire s'il admet une représentation sagittale dans un plan sans que les arêtes se croisent.
Quand les graphes deviennent plus complexes, le problème de décision est NP-complet mais le problème d'optimisation est NP-dur.

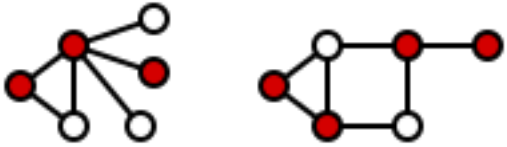
Le problème MIS

Étant donné un graphe G on peut définir un *ensemble indépendant* (ou *independant set*) par un sous-ensemble S de sommets de G tel qu'il n'existe aucune arête qui relit deux éléments de S.
Il existe souvent plusieurs solutions à ce problème.
Les MIS sont des *sous-ensembles dominants*. On dit qu'un sous-ensemble D d'un graphe G est dominant si chaque sommet de G est soit un élément de D, soit dispose d'un voisin dans D (donc il existe une arête qui le relie à un élément de D) s'il n'est pas dans D. Les MIS sont les plus grands sous-ensembles dominants.



Le problème MVC

Le problème MVC, acronyme de *Minimum Vertex Cover*, ou *problème de couverture par sommets*, est un problème dual du problème MIS.
Une couverture par sommets, aussi appelée *transversal* d'un graphe G est un ensemble C de sommets tel que chaque arête de $G = (V, E)$ est incidente à au moins un sommet de C, C'est à dire un sous-ensemble de sommets $S \subseteq V$ tel que pour chaque arête (u, v) de G on a $u \in S$ ou $v \in S$. On dit que l'ensemble C couvre les arêtes de G.



Le problème SAT 1/2

Le problème SAT ou le *problème de satisfaisabilité booléenne* est un problème de décision. Étant donné des variables booléennes (qui prennent les valeurs *vrai* ou *faux*) et une proposition, c'est-à-dire une formule qui combine ces variables avec des opérateurs booléens, on cherche à savoir s'il existe une combinaison de valeurs des variables qui rende vraie cette proposition .
Par exemple, la proposition $(p \wedge q) \vee \neg p$ est vraie pour toutes valeurs de q si p a la valeur *faux*, de même la proposition $(p \wedge \neg p)$ ne peut être satisfaite par aucune valeur de p.
Le problème SAT est l'archétype même des problèmes NP-complets. On peut identifier différentes formes simplifiées de SAT. vant d'aller plus loin, on doit définir ce qu'est une *Forme Normale Conjonctive*, ou CNF [2]. Une conjonction est une opération "AND", une forme normale conjonctive est une équation booléenne qui est une évaluation d'une succession de clauses qui ne contiennent pas de AND.

2. en anglais l'acronyme devient *Conjunctive Normal Form*

Le problème SAT 2/2

Une CNF est donc de la forme $(clause1) \wedge (clause2) \wedge \cdots \wedge (clauneN)$. Chaque clause est elle-même de la forme $a \vee \cdots b$ avec éventuellement des négations $\neg v$. Une CNF s'écrit donc

$$\bigwedge_{i=1}^{p} (\bigvee_{j=1}^{q} l_{ij}) \text{ avec } l_{ij} = a_{ij} \text{ ou } l_{ij} = \neg a_{ij}$$

Les simplifications les plus courantes du problème SAT sont :

- le problème **CNF-SAT** correspond au cas où la proposition est une CNF ;
- le problème **3-SAT** est une restriction de CNF-SAT où chaque clause comporte au plus 3 variables ;
- le problème **2-SAT** est une restriction de CNF-SAT où chaque clause comporte au plus 2 variables.

Le problème 2-SAT est de complexité P, mais 3-SAT est de difficulté NP.
On peut montrer que le problème SAT se ramène toujours au problème 3-SAT.
Le problème SAT est la base de la démonstration du théorème de Cook.

Le problème QUBO 1/2

L'acronyme *QUBO* signifie *Quadratic Unconstrained Binary Optimisation*. Il permet de résoudre des problèmes d'optimisation qui se ramènenent, dans les grandes lignes, à la recherche d'optima d'une forme quadratique.
Etant donnée un entier $n \in \mathbb{N}$, étant donné $\mathbb{B}^n = \{0; 1\}n$, l'ensemble des vecteurs de taille n formés de 0 et de 1, étant donné une forme quadratique f_Q représentée par une matrice $Q \in n\mathbb{R}^{n \times n}$, quel est la valeur $x^* \in \mathbb{B}^n$ qui minimise $f_Q(x) = x^T.Q.x$
Le problème QUBO possède différentes propriétés :

- multiplier Q par un facteur α ne change pas l'optimum ;
- inverse le signe de Q (mettre un moins devant) revient à chercher un maximum plutôt qu'un minimum ;
- si Q est une matrice diagonale, le problème est trivial également, le bit de rang i sera 0 si Q_{ii} est positif et 1 sinon ;

Le problème QUBO 2/2

D'une manière générale, on ajoute parfois au terme quadratique un terme linéaire, l'énoncé devient alors

$$Q \in \mathbb{R}^{n \times n}, c \in \mathbb{R}^n, \text{ trouver la valeur } x^* \text{ qui minime } f(x) = x^T.Q.x + c^T.x$$

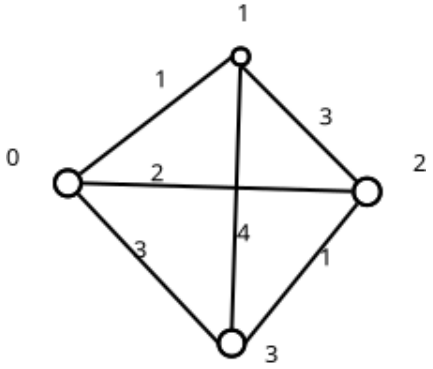
Le problème QUBO trouve des applications dans de nombreux domaines, car il est bien adapté à la recherche d'un optimum. Il intéresse ainsi les domaines de la finance, de l'économie, mais aussi la logistique etl'intelligence artificielle.
Le problème QUBO est de nature NPC

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Résoudre MaxCut avec QUBO 1/3

Considérons le graphe suivant, il dispose de 4 noeuds, numérotés de 0 à 4, les arêtes portent différents poids allant de 1 à 4.
Ainsi,l'arête entre les noeuds 1 et 4 porte le poids 4 et celle entre 2 et 3 le poids 1.



Résoudre MaxCut avec QUBO 2/3

On peut traduire ce graphe par une "matrice de connectivité" W dont les coefficients w_{ij} sont

- 0 si $i = j$
- le poids de l'arête entre i et j si $i \neq j$

Dans notre exemple, on va construire la matrice suivante

$$W = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 4 \\ 2 & 3 & 0 & 1 \\ 3 & 4 & 1 & 0 \end{pmatrix}$$

Dans le cadre du problème MaxCut, on cherche une coupe maximale, donc un sous-ensemble E des nœuds du graphe qui maximise la coupe.
Connaissant E, on peut associer au noeud de rang i la valeur 1 s'il est dans E et 0 sinon. Cela nous permet de construire un vecteur x de valeur binaire. Inversement, un vecteur binaire $x \in \mathbb{B}^4$ décrit parfaitement une coupe.

Résoudre MaxCut avec QUBO 3/3

Considérons à présent la fonction de coût suivante qui représenté par un vecteur binaire x

$$x \in \mathbb{B}^4, C(x) = \sum_{i,j} W_{ij} x_i (1 - x_j)$$

- x_i est non nul si le noeud i est dans E
- $1 - x_j$ est non nul si le noeud i **n'est pas** dans E
- le terme $x_i(1 - x_j)$, qui est associé à l'arête entre i et j, sera non nulle si cette arête est dans la coupe, donc si elle relie deux points dans E et hors de F
- on fait donc la somme des poids W_{ij} des arêtes dans la coupe, les autres termes sont nuls.

$$c \in \mathbb{R}^4, c_i = \sum_j W_{ij} \text{ et } Q = -W, \forall i, j Q_{ij} = -W_{ij}$$

$$C(x) = \sum_{i,j} W_{ij} x_i (1 - x_j) = C(x) = -\sum_{i,j} W_{ij} x_i x_j) + \sum_i c_i . x_i = x^T . Q . x + c^T . x$$

ce qui est la formulation classique du QUBO

MIS et MVC se ramènent au QUBO 1/2

Le problème MVC, donc le problème MIS, peuvent s'exprimer sous la forme d'un QUBO.
Considérons MVC, pour définir une couverture par sommet, on va associer une valeur binaire x_i au sommet de rang i selon que le nœud est dans la couverture ou non.
Formellent, cela revient à minimiser la somme des x_i en garantissant que pour chaque arête de E, entre les noeuds i et j, au moins l'un des deux est dans la couvertures donc
$x_i + x_j \geq 1, \forall (i,j) \in E$
La méthode classiquement utilisée pour exprimer la contrainte consiste à ajouter un terme de "pénalité" qui va augmenter la fonction de coût dans les cas où la contrainte n'est pas réalisée.
Considérons le terme suivant

$$x \in \{0;1\}, y \in \{0;1\}, penalite(x,y) = 1 - x - y + xy$$

On peut identifier les cas suivants selon les valeurs de x et y

MIS et MVC se ramènent au QUBO 2/2

x	y	x+y	xy	1-x-y+xy	contrainte réalisée ?
0	0	0	0	1	NON
0	1	1	0	0	OUI
1	0	1	0	0	OUI
1	1	2	1	0	OUI

L'expression $1 - x - y + xy$ traduit donc la réalisation ou non de la contrainte $x + y \geq 1$. On va donc construire la fonction de coût suivante à minimiser

$$C(x) = \sum_i x_i + \sum_{i,j} (1 - x_i - x_j + x_i x_j)$$

Il est classique d'ajouter le paramètre P, un réel positif, pour accélérer la convergence

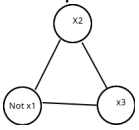
$$C_P(x) = \sum_i x_i + \sum_{i,j} P.(1 - x_i - x_j + x_i x_j) = (1 - 2P) \sum_i x_i + P \sum_{i,j} x_i.x_j$$

Le problème 3-SAT est un problème de type QUBO 1/2

Le problème 3-SAT, peut être résolu à l'aide d'un QUBO. La procédure consiste à traduire la formulation de 3-SAT en un roblème de graphe de type MIS qui peut être lui-même transformé en QUBO.
Considérons une CNF qui comprend n variables et m clauses.

- pour chaque clause, on construit un petit graphe à 3 sommets, chaque sommet étant une variable ou la négation d'une variable ;
- chacun de ses "sous-graphes"[3], est connecté en raccordant les nœuds qui représentent une variable et sa négation.

Par exemple, la clause $\neg x_1 \vee x_2 \vee x_3$ sera représentée par le graphe de la figure suivante

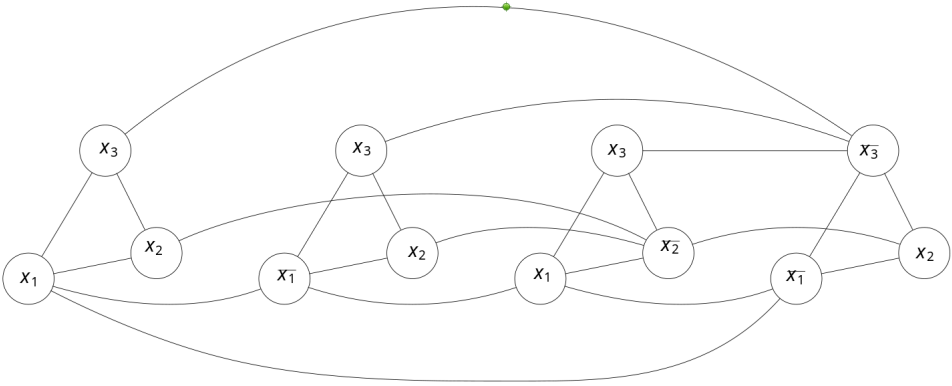


3. un tel sous-graphe est désigné sous le nom de *clique*

Le problème 3-SAT est un problème de type QUBO 2/2

On interconnecte ensuite les sous-graphes en reliant les variables et leurs négations.
Considérons la CNF suivante

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3)$$



Problème 3-SAT via QUBO/MIS

On peut démontrer que la résolution du problème MIS sur ce graphe permet de trouver une solution maximale de la clause correspondante. Si la taille de ce MIS est égale au nombre de clauses dans la CNF, alors celle-ci peut être satisfaite.

On rappelle que SAT veut savoir si une clause peut oui ou non être satisfait, mais ne cherche pas forcément une combinaison de variables booléennes qui satisfasse. SAT cherche juste à savoir si une telle solution existe.

Si la taille du MIS trouvée est inférieure au nombre de clauses, alors la CNF ne peut pas être satisfaite.

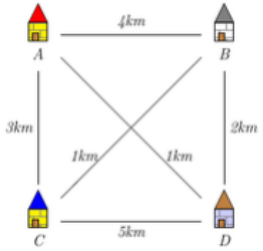
Le problème du voyageur de commerce est un QUBO 1/2

Le *TSP* ou *Traveling Salesperson Problem*, ou *problème du voyageur de commerce* est un problème très classique en recherche opérationnelle. Il s'agit d'optimiser la tournée d'un véhicule qui effectue sa tournée entre son dépôt et différents clients situés dans un réseau routier.

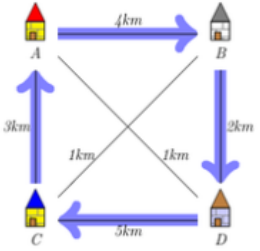
Etant donné n villes et les distances entre toutes les paires de villes, trouver un chemin de longueur totale minimale qui passe exactement une fois par chaque ville et revienne à la ville de départ.

On modélisera TSP comme un problème sur un graphe non orienté pondéré où les villes sont définies comme les sommets du graphe et où les chemins entre les villes, parcourues par le voyageur de commerce, sont les arêtes. Le coût d'une arête entre deux sommets est la distance entre les deux villes correspondantes.

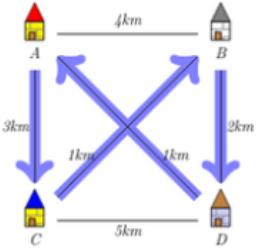
Le problème du voyageur de commerce est un QUBO 2/2



(a) Instance du problème



(b) Solution triviale et mauvaise



(c) Solution optimale

Fonction de coût de TSP/QUBO 1/3

Il est possible de formuler le TSP sous la forme d'un QUBO en considérant un ensemble de villes numérotées de 1 à N, on définira le coefficient x_{ij} tel que $x_{ij} = 1$ s'il existe une route entre la ville de rang i et la ville de rang j, sinon $x_{ij} = 0$.

Les coefficients x_{ij} permettent de définir un graphe dans lesquels les villes sont les sommets, on empruntera la route entre i et j si $x_{ij} = 1$. On associe un poids à l'arête ij qui correspond au temps de parcours entre les deux villes, cela permet la définition d'un coefficient de coût C_{ij}

Il existe différentes manières de formaliser TSP, voici l'une d'entre elles où résoudre TSP revient à minimiser la fonction binaire sur le vecteur x

$$C^A(x) = \sum_{i}^{N} \sum_{j=1, j\neq i}^{N} C_{ij} x_{ij} = 1$$

Fonction de coût de TSP/QUBO 2/3

On note qu'on évite les cas $i = j$, puisqu'un voyage entre deux villes implique forcément des villes différentes. On doit également ajouter les contraintes suivantes

$$\forall i \in \{1, 2, \cdots, N\} \sum_{j=1, j\neq i}^{N} x_{ij} = 1$$

qui traduit le fait qu'il n'existe, dans la tournée du voyageur de commerce, qu'un seul passage par la ville de rang i, on ici chercher à minimiser la fonction de coût suivante

$$\forall i \in \{1, 2, \cdots, N\}, C_i^B(x) = \sum_{j=1, j\neq i}^{N} (1 - x_{ij})^2$$

Fonction de coût de TSP/QUBO 3/3

Par ailleurs, on doit traduire le fait que pour tout ensemble de villes, il existe toujours au moins une route qui part de l'une d'entre elles pour aller dans une ville qui n'appartient pas à cet ensemble, soit

$$\forall S \subseteq \{1, 2, \cdots, N\}, S \neq \emptyset, \sum_{i \in S} \sum_{j \in \{1,2,\cdots,N\} \setminus S} x_{ij} \geq 1$$

Ce qui revient à minimiser la fonction

$$\forall S \subseteq \{1, 2, \cdots, N\}, S \neq \emptyset, C_S^C(x) = \sum_{i \in S} \sum_{j \in \{1,2,\cdots,N\} \setminus S} (x_{ij} - 1)$$

La fonction de coût de TSP est un QUBO

La fonction de coût va se construire la fonction de coût total en effectuant deux actions :

- réunir les x_{ij} sur une seule dimension, en mettant les "lignes" de la forme $x_{i1}x_{i2}\cdots x_{iN}$ les unes en dessous des autres et en effectuant le changement de variables correspondant dans les équations ci-dessus,
- en construisant une fonction de coût global comme la somme des fonctions de coût précédentes.

La fonction qui en résulte est de la forme

$$C^T(x) = \sum_{i,j=1}^{N} Q_{ij}x_i x_j + \sum_{i=1}^{N} C_i x_i = x^t.Q.x + C^t.x$$

qui correspond à la forme générique d'un problème QUBO.

QUBO et ses amis : conclusion partielle

Le problème QUBO semble au centre des algorithmiques présentées. Le fait qu'il soit "presque résoluble" par du HPCn depuis 1983 n'y est pas étranger.

D'autres problèmes NPC sont également intéressants, tels que MIS ou MWIS.

Passer d'un problème NP à un problème NPC est toujours de complexité P (théorème de Cook), mais trouver cette procédure est **très** compliqué.

QUBO est implémenté matériellement par les *Quantum Annealers* du constructeur **D-Wave**

On verra que le problème MIS est au coeur des ordinateurs analoique du constructeur **Pasqal**

Plan

28 Un petit détour par la théorie de la complexité

29 Zoologie de Karp des problèmes NPC

30 Éléments de physique et théorème adiabatique

31 Quelques problèmes classiques

32 QUBO et les autres problèmes NPC

33 Machine Pasqal et problème MIS

34 VQE

35 QAOA

36 Inégalités de Bell

37 Le jeu CHSH

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Principe de VQE - Variationnal Quantum Eigensolver

On considère que l'on dispose d'un hamiltonien H, représentatif d'un problème d'optimisaton ou d'un problème de chimie quantique.

On se place ici dans le contexte de la résolution de l'équation de Schrödinger indépendante du temps. Celle-ci va s'exprimer sous la forme

$$H|\Psi\rangle = E|\Psi\rangle$$

Il s'agit en l'occurrence de trouver les valeurs propres et les vecteurs propres de H (les valeurs propres sont réelles, puisque H est un hamiltonien donc une matrice hermitienne).

Les vecteurs propres correspondent aux états propres de l'hamiltonien, parmi eux, il y a une valeur propre de valeur minimale, notée E_0, qui correspond à l'état de base de l'hamiltonien.

Valeurs propres de l'hamiltonien

Si $|\Psi_i\rangle$ est le i-ème vecteur propre associé à la valeur propre E_i, on peut évaluer l'énergie du système définie par

$$\langle\Psi| H |\Psi\rangle$$

Sur les vecteurs propres on remarque que

$$\forall i \text{ état propre de H }, H|\Psi_i\rangle = E_i|\Psi_i\rangle \text{ donc } \langle\Psi_i| H |\Psi_i\rangle = E_i \langle\Psi_i||\Psi_i\rangle = E_i$$

Par conséquent

$$\langle\Psi_i| H |\Psi_i\rangle = E_i \geq E_0 = \langle\Psi_0| H |\Psi_0\rangle$$

Par linéarité, il apparaît que $\langle\Psi| H |\Psi\rangle$ est toujours minoré par E_0.

Valeur propre minimum et orthogonalité

En effet, soit $(|\phi_i\rangle)$, une base de vecteur propres de l'hamiltonien H. Soit λ_{min} la plus petite valeur propre et $|\phi_{min}\rangle$ le vecteur propre associé. Pour tout vecteur $|\psi\rangle$, on a

$$|\psi\rangle = \alpha\,|\phi_{min}\rangle + \beta\,|\phi_{other}\rangle$$

Le vecteur $|\phi_{min}\rangle$ et $H\,|\phi_{other}\rangle$ sont orthogonaux, en effet $|\phi_{other}\rangle$ est une combinaison de vecteurs propres qui ne sont pas $|\phi_{min}\rangle$ et donc

$$\langle\phi_{min}|\,H\,|\phi_{other}\rangle = \sum_{j\neq min} \alpha_j\,\langle\phi_{min}|\,H\,\left|\phi_j\right\rangle = \sum_{j\neq min} \alpha_j\lambda_j\,\langle\phi_{min}|\,\left|\phi_j\right\rangle = \sum_{j\neq min} \alpha_j\lambda_j.0 = 0$$

La valeur propre minimale est le minimum

Si $|\psi\rangle = \alpha |\phi_{min}\rangle + \beta |\phi_{other}\rangle$ alors

$$\begin{aligned}
\langle\psi| H |\psi\rangle &= (\alpha^* \langle\phi_{min}| + \beta^* \langle\phi_{other}|) H (\alpha |\phi_{min}\rangle + \beta |\phi_{other}\rangle) \\
&= |\alpha|^2 \langle\phi_{min}| H |\phi_{min}\rangle + \alpha\beta^* \langle\phi_{other}| H |\phi_{min}\rangle + \alpha^*\beta \langle\phi_{min}| H |\phi_{other}\rangle + |\beta|^2 \langle\phi_{other}| H |\phi_{other}\rangle \\
&= |\alpha|^2 \lambda_{min} \langle\phi_{min}|\phi_{min}\rangle + \alpha\beta^* \lambda_{min} \langle\phi_{other}|\phi_{min}\rangle + 0 + |\beta|^2 \langle\phi_{other}| H |\phi_{other}\rangle \\
&= |\alpha|^2 \lambda_{min} + |\beta|^2 \langle\phi_{other}| H |\phi_{other}\rangle
\end{aligned}$$

Or

$$\langle\phi_{other}| H |\phi_{other}\rangle = \sum_{j\neq min} \sum_{k\neq min} \alpha_k^* \alpha_j \langle\phi_k| H |\phi_j\rangle = \sum_{j\neq min} \sum_{k\neq min} \lambda_j \alpha_k^* \alpha_j \langle\phi_k|\phi_j\rangle = \sum_{j\neq min} |\alpha_j|^2 \lambda_j \geq \lambda_{min} \sum_{j\neq min} |\alpha_j|^2$$

Mais puisque $|\alpha|^2 + \sum_{j\neq min} |\alpha_j|^2 = 1$ (condition de normalisation)

$$\langle\psi| H |\psi\rangle = |\alpha|^2 \lambda_{min} + |\beta|^2 \langle\phi_{other}| H |\phi_{other}\rangle \geq |\alpha|^2 \lambda_{min} + \lambda_{min} \sum_{j\neq min} |\alpha_j|^2 = \lambda_{min}(|\alpha|^2 + \sum_{j\neq min} |\alpha_j|^2) = \lambda_{min}$$

Construite l'hamiltonien

La physique nous informe que l'hamiltonien peut toujours s'écrire comme une **somme** d'opérateurs de Pauli effectués sur un ou plusieurs qubits.

$$H = h_I I + \sum_i h_i A_i + \sum_{i,j} h_{ij} A_i A_j + \sum_{i,j,k} h_{ijk} A_i A_j A_k + \cdots$$

où A_i est un opérateur X, Y ou Z appliqué sur le qubit de rang i

Par exemple

$$CNOT = \frac{1}{2}(I \otimes I + Z \otimes I + I \otimes I - Z \otimes X)$$

Pour calculer $\langle\psi| H |\psi\rangle$ il suffit de savoir calculer $\langle\psi| A_i |\psi\rangle$, $\langle\psi| A_i A_j |\psi\rangle$, $\langle\psi| A_i A_j A_k |\psi\rangle$, ...

Calculer les termes de l'hamiltonien

On va voir comment les mesures permettent d'évaluer les produits scalaires

Si $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, on a $Pr(|0\rangle) = |\alpha|^2$

Or $\alpha = \langle 0|\psi\rangle$, donc $Pr(|0\rangle) = |\langle 0|\psi\rangle|^2 = (\langle 0|\psi\rangle)^* \langle 0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \langle\psi|(\langle 0|0\rangle)|\psi\rangle$

De même $Pr(|1\rangle = |\langle 1|\psi\rangle|^2 = \langle\psi|(\langle 1||1\rangle))|\psi\rangle$

Coup de projecteurs sur I, X, Y et Z

Il est évident que

- $I = |0\rangle\langle 0| + |1\rangle\langle 1|$
- $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$

On sait que $Z = HZH$, donc

$$\langle\psi| X |\psi\rangle = \langle\psi| HZH |\psi\rangle = \langle H\psi| Z |H\psi\rangle$$

Il suffit de s'intéresser à $H|\psi\rangle$ au lieu de $ket\psi$

De même on a $Y = SHZHS^\dagger$, don le cas Y on va travailler sur $HS^\dagger|\psi\rangle$

Passage à plusieurs qubits

Il est possible de mesurer le produit scalaire aussi dans le cas où plusieurs qubits sont mis en jeu.
Soit par exemple 3 qubits et $Z_0Z_1 = Z \otimes Z \otimes I$

$$\begin{aligned}\langle\psi| Z_0Z_1 |\psi\rangle &= \langle\psi| Z \otimes Z \otimes I |\psi\rangle = \langle\psi| \left(\langle 0||0\rangle - \langle 1||1\rangle\right) \otimes \left(\langle 0||0\rangle - \langle 1||1\rangle\right) \otimes I |\psi\rangle \\ &= \langle\psi||00\rangle\langle 00| \otimes I |\psi\rangle - \langle\psi||01\rangle\langle 01| \otimes I |\psi\rangle - \langle\psi||10\rangle\langle 10| \otimes I |\psi\rangle + \langle\psi||11\rangle\langle 11| \otimes I |\psi\rangle \\ &= Pr(|00x\rangle) - Pr(|01x\rangle - Pr(|10x\rangle + Pr(|11x\rangle\end{aligned}$$

où $Pr(|00x\rangle)$ est la probabilité de mesurer $|0\rangle$ sur les deux premiers qubits en ignorant la valeur du dernier qubit.

En mettant des Z, H, S sur les lignes des qubits, et des mesures, on peut évaluer $\langle\psi| H |\psi\rangle$

Principe de VQE

Le principe de VQE se base sur ce constat : on crée un $\left|\Psi(\theta)\right\rangle$ paramétré, ou *anstaz* qui permet de construire une fonction de coût qu'on va chercher à minimiser pour trouver une valeeur approximative de E_0. Sans surprise, la fonction de coût sera de la forme

$$C(\theta) = \left\langle \Psi(\theta) \right| H \left| \Psi(\theta) \right\rangle$$

L'optimeur classique, qui tourne sur du HPC, va chercher à minimiser la veleur de la fonction de coût en fonction du paramètre de l'ansatz.

On est là pleinement dans une approche hybride HPC/QC

Construction de l'ansatz

L'ansatz $\left|\Psi(\theta)\right\rangle$ est construit à partir d'un état de base auquel on applique une transformation unitaire elle-même paramétrée par θ

$$\left|\Psi(\theta)\right\rangle = U(\theta)\left|\Psi_{HD}\right\rangle, \forall\theta, U(\theta) \text{ est unitaire}$$

Le paramètre θ est généralement un p-uplet de valeurs réelles

$$\theta = (\theta_1, \theta_2, \cdots, \theta_p)$$

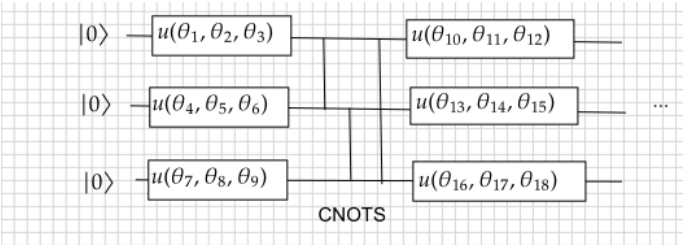
L'opérateur $U(\theta)$ sera composé d'opérateurs simples, en général des portes à un oou deux qubits, agissant sur les n qubits du problème.

$$U(\theta) = U_1(\theta_1)U_2(\theta_2)\cdots U_p((\theta_p)$$

Circuit implémentant l'ansatz

On va construire un circuit qui implémente l'opérateur U paramétré qui fait varier $|\psi\rangle$ en combinant des rotations paramétrés sur X, Y et Z ainsi que des CNOTS pour induire de l'intrication

Par exemple sur 3 qubits on va avoir un circuit qui ressemblera à ceci. Tout le "savoir faire" de VQE consiste à construire un circuit qui accélère la convergence de l'algorithme.



Fonctionnement de VQE

Le fonctionnement de VQE peut se décrire simplement par

1. à la k-ième itération, on a un jeu de paramètres θ^k
2. on construit un circuit paramétré qui représente $U(\theta^k)$
3. on calcule $\left|\Psi(\theta^k)\right\rangle$ et la valeur de la fonction de coût $C(\theta^k)$
4. on injecte cette valeur dans l'optmiseur qui produit une nouvelle valeur de paramètre θ^{k+1}
5. on reboucle jusqu'à obtenir une valeur jugée pertinente par l'optimiseur.

Opérateur unitaire dans VQE

C'est dans la construction de cet opérateur U que réside tout le savoir faire de mise en oeuvre de VQE, et tout affaire de compromis :

- les portes U_i sont des portes à 1 ou 2 qubits
- les circuits sont peu profonds pour être peu sensibles au bruit et à la décohérence
- le nombre de paramètres θ_i doit être assez grand pour construire un espace de recherche de solutions qui soit assez grand, en particulier il n'est pas acquis que la valeur cible E_0 soit dans cet espace, parfois on obtiendra qu'une valeur approchée.
- le nombre de paramètres θ_i ne doit paas être gros grand pour que l'optimiseur HPC reste efficace et fournisse une solution pertinente.

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Quantum Approximate Optimization Algorithm

L'algorithme *Quantum Approximate Optimization Algorithm* ou **QAOA** appartient à la famille des algorithmes variationnels.

Il utilise des phases HPC et des phases QC, c'est un représentant typique des algorithmes hybrides actuels qui fonctionnent sur des qubits et des portes bruités et imparfaits.

Dans les grandes lignes QAOA c'est

- une émulation, avec des circuits à portes quantiques, d'un *annealer* adiabatique
- des circuits quantiques construits itérativement, et optmisés par du HPC, c'est l'approche **variationelle**

ATTENTION !!! On retrouvera ici les opérateurs X, Y, Z des portes classiques, car ils permettent aux physiciens de décrire facilement des hamiltoniens.
Il ne faut pas confondre les hamiltoniens avec les transformations unitaires des circuits quantiques (lesquels sont des exponentielles de sommes et d'intégrales d'hamiltoniens).

Back to Schrödinger

L'équation de Schrödinger s'écrit ainsi

$$i\hbar\frac{\partial}{\partial t}\left|\Psi(x,t)\right\rangle = -\frac{\hbar^2}{2m}\nabla^2\left|\Psi(x,t)\right\rangle + V(x,t)\left|\Psi(x,t)\right\rangle.$$

Si j'ai déjà identifié un hamiltonien, elle va s'écrire

$$i\hbar\frac{\partial}{\partial t}\left|\Psi(t)\right\rangle = H\left|\Psi(t)\right\rangle.$$

que je peux encore simplifier en cachant la constante de Planck dans H

$$i\frac{\partial}{\partial t}\left|\Psi(t)\right\rangle = H\left|\Psi(t)\right\rangle.$$

Par conséquent, la solution peut s'écrire

$$\left|\Psi(t)\right\rangle = U(t)\left|\Psi(0)\right\rangle \text{ avec } U(t) = e^{i\int_0^t H(t)dt}$$

Discrétisation de l'opérateur unitaire

Si on se positionne sur une période ΔT assez courte, il est possible de découper $U(t)$ en petits morceaux

$$U(t) = e^{i\int_0^t H(t)dt} = U(T, T-\Delta T)U(T-\Delta T, T-2\Delta T\cdots U(\Delta T, 0)$$

avec

$$U(j\Delta T, (j-1)\Delta T) = e^{i\int_{(j-1)\Delta T}^{j\Delta T} H(t)dt} \approx e^{iH(j\Delta T)\Delta T} \text{ si } \Delta T \text{ est assez petit}$$

On considère que l'exponentielle est pratiquement constante sur l'intervalle de largeur ΔT. On peut donc en déduire que

$$U(T, 0) \approx \prod_{j=0}^{p} e^{iH(j\Delta T)\Delta T}$$

Utilisation de la décomposition de Trotter-Suzuki

Il s'agit maintenant que simplifier ce produit d'exponentielle, attendu que les $iH(j\Delta T$ ne commutent pas a priori. C'est ici que la formule de Trotter vient à notre secours, en effet, elle peut s'écrire sous la forme

$$e^{i(A+B)t} = e^{iAt} + e^{iBt} + O(t^2)$$

On rappelle que l'hamiltonien dépendant du temps s'écrit

$$H(t) = (1 - s(t))H_P + s(t)H_B, s(t = 0) = 0, s(t = T) = 1$$

En regroupant tous les termes on obtient

$$\begin{aligned} U(T,0) &\approx \prod_{j=0}^{p} e^{iH(j\Delta T)\Delta T} \\ &= \prod_{j=0}^{p} e^{i(1-s(j\Delta T))H_P(\Delta T)+s(\Delta T)H_B(\Delta T))\Delta T} \\ &\approx \prod_{j=0}^{p} e^{i(1-s(j\Delta T))H_P(\Delta T)\Delta T} e^{i(s(\Delta T)H_B(\Delta T))\Delta T} \end{aligned}$$

Construction d'un ansatz 1/2

Dans le but de pouvoir introduire un optimiseur classique, on commence à construire un ansatz, c'est à dire une paramétrisation de notre problème par des réels.

$$U(T,0) \approx \prod_{j=0}^{p} e^{i(1-s(j\Delta T))H_P(\Delta T)\Delta T} e^{i(s(\Delta T)H_B(\Delta T))\Delta T}$$

On a donc un produit de tronçons de la forme

$$U_j = e^{i(1-s(j\Delta T))H_P(\Delta T)\Delta T} e^{i(s(\Delta T)H_B(\Delta T))\Delta T}$$

En se rappelant que

$$H_B = -\sum_j X_j$$

On rappelle que les portes X_j commutent.

Construction d'un ansatz 2/2

Nous introduisons p couples de paramètres γ_j et β_j en posant

$$\beta_j = -[1 - s(j\Delta T)]\Delta T$$
$$\gamma_j = -s(j\Delta T)\Delta T$$

Le tronçon peut alors se réécrire ainsi

$$U_j = e^{-i\gamma_j H_P} e^{-i\gamma_j H_B}$$

L'ansatz sera constitué des p couples de paramètres (β_j, γ_j). En partant de l'état fondamentale de H_B qui est $|+\rangle^{\otimes n}$, on peut construire un vecteur paramétré

$$\left|\Phi(\beta,\gamma)\right\rangle = (\prod_{j=0}^{p} U_j) H^{\otimes n} |0\rangle = (\prod_{j=0}^{p} e^{-i\gamma_j H_P} e^{-i\gamma_j H_B}) H^{\otimes n} |0\rangle$$

Constrction d'un circuit pour chaque étape

Il s'agit maintenant de construire un circuit qui représente l'opérateur $QAOA(\beta, \gamma)$

$$QAOA(\beta, \gamma) = \prod_{j=0}^{p} e^{-i\gamma_j H_P} e^{-i\gamma_j H_B}) H^{\otimes n}$$

On rappelle les rotations paramétrées sur les qubits

$$R_X(\theta) = e^{-i\theta/2X} = \begin{pmatrix} cos(\theta/2) & -isin(\theta/2) \\ isin(\theta/2) & cos(\theta/2) \end{pmatrix}$$

$$R_Y(\theta) = e^{-i\theta/2Y} = \begin{pmatrix} cos(\theta/2) & sin(\theta/2) \\ sin(\theta/2) & cos(\theta/2) \end{pmatrix}$$

$$R_Z(\theta) = e^{-i\theta/2Z} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

L'expression $QAOA(\beta, \gamma)$ est formée d'exponentielle selon X, Y et Z, donc de portes paramétrées $e^{-iPt} = R_P(2t), P \in \{X, Y, Z\}$ et de termes de la portes $P_i P_j \cdots, P \in \{X, Y, Z\}$ qui appliquent des portes X, Y et Z sur plusieurs qubits à la fois.

Double porte Z

Considérons la porte $Z_1 Z_2 = Z \otimes Z$ sur deux qubits

$$
\begin{aligned}
e^{-iZ\otimes Zt} |00\rangle &= e^{-i(1\times 1)t} |00\rangle = e^{-it} |00\rangle \\
e^{-iZ\otimes Zt} |01\rangle &= e^{-i(1\times -1)t} |01\rangle = e^{it} |01\rangle \\
e^{-iZ\otimes Zt} |10\rangle &= e^{-i(-1\times 1)t} |10\rangle = e^{-t} |10\rangle \\
e^{-iZ\otimes Zt} |11\rangle &= e^{-i(-1\times -1)t} |11\rangle = e^{-it} |11\rangle
\end{aligned}
$$

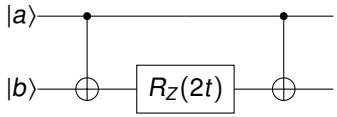
D'une manière synthétique, on peut écrire

$$\forall (a,b) \in \{0,1\}^2, e^{-iZ\otimes Zt} |ab\rangle = e^{-i(-1)^{a\oplus b} t} |ab\rangle$$

Ou la notion $\oplus$ représente le XOR booléean.

Circuit de la porte double Z

Ce résultat peut s'implémenter grâce au circuit quantique suivant



En effet, ce circuit produit l'effet suivant

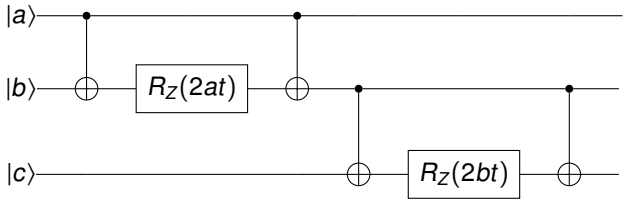
- on commence à l'état $|a\rangle\,|b\rangle$
- le premier CNOT produit $|a\rangle\,|a \oplus b\rangle$
- la rotation paramétrée produit $|a\rangle \left|e^{-i(-1)^{a\oplus b}t}\, a \oplus b\right\rangle = e^{-i(-1)^{a\oplus b}t}\,|a\rangle\,|a \oplus b\rangle$
- le second CNOT opère sur $|a\rangle\,|a \oplus b \oplus a\rangle = |a\rangle\,|b\rangle = |ab\rangle$
- le résultat final est alors $e^{-i(-1)^{a\oplus b}t}\,|ab\rangle$

Simplification

Les Z_iZ_j commutent, par conséquent on peut simplifier certaines expressions avec le circuit suivant

$$e^{-iaZ_iZ_jt-ibZ_jZ_kt} = e^{-iaZ_iZ_jt}e^{-ibZ_jZ_kt}$$

Ce qui correspond au circuit



En appliquant cette démarche pour les autres types de portes, on va construire itérativement, pour chaque terme de l'opérateur $QAOA(\beta, \gamma)$, une couche de circuit. On peut ainsi construire, pour chaque valeurs de paramètres (β, γ) un circuit d'autant plus profond que p, le nombre de paires de paramètres, est grand.

Minimiser l'énergie avec un optimiseur

On est désormais en mesure de calculer l'état $\left|\Phi(\beta,\gamma)\right\rangle$, ou ansatz, avec un circuit quantique. L'énergie qui correspond est donnée par

$$E(\beta,\gamma) = \left\langle \Phi(\beta,\gamma)\right| H_P \left|\Phi(\beta,\gamma)\right\rangle$$

Où H_P représente l'hamiltonien du problème, c'est à dire la fonction que l'on cherche à minimiser. Cette énergie paramétrée par (β,γ) représente une fonction de coût qui peut être minimisée par un optimiseur comme par exemple COBYLA.

QAOA : conclusion et résumé

Le fonctionnement de QAOA sera donc le suivant :

1. on part d'un premier jeu de paramètres (β_0, γ_0)
2. on construit le circuit quantique qui correspond, on s'en sert pour calculer $\left|\Phi(\beta,\gamma)\right\rangle$
3. on peut évaluer la fonction de coût $\left\langle\Phi(\beta,\gamma)\right| H_P \left|\Phi(\beta,\gamma)\right\rangle$
4. l'optimiseur produit un nouveau jeu de paramètres (β_i, γ_i)
5. on recommence jusqu'à ce que l'optimiseur converge

Plan

28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Approche ensembliste

Considérons des enfants dans une cour de récréation pendant l'hiver On peut représenter les populations comme suit :

- A : les enfants qui portent des écharpes
- B : les enfants qui portent des bonnets
- C : les enfants qui portent des lunettes

Mettons les choses en équation. On notera

- A^+ est la population avec écharpe
- A^- est la population sans écharpe
- B^+ est la population avec bonnet
- B^- est la population sans bonnet
- C^+ est la population avec lunettes
- C^- est la population sans lunette

On note A^+B^- la population composée des gens avec écharpe et sans bonnet, et $A^+B^-C^+$ celle des enfants avec écharpes et lunettes mais sans bonnet.

Inégalités ensemblistes

Si je considère l'ensemble A^+B^+ des enfants qui ont à la fois des écharpes et des bonnets, je vais y trouver deux sous-gropes distants parmi eux : ceux qui ont des lunettes (qui sont dans $A^+B^+C^+$) et ceux qui n'en ont pas (les éléments de $< A^+B^+C^- >$), on a donc

$$A^+B^+ = A^+B^+C^+ \cup A^+B^+C^-$$

Mais on a aussi

$$B^+C^+ = A^+B^+C^+ \cup < A^-B^+C^+ > \text{ donc } A^+B^+C^+ \subseteq B^+C^+$$
$$A^+C^- = A^+B^+C^- \cup < A^+B^-C^+ > \text{ donc } A^+B^+C^- \subseteq A^+C^-$$

Par conséquent

$$A^+B^+ = A^+B^+C^+ \cup A^+B^+C^- \subseteq A^+C^- \cup B^+C^+$$

Cardinaux et probabilités

On rapportant aux cardinaux des ensembles on aura

$$A^+B^+ \subseteq A^+C^- \cup B^+C^+ \text{ donc } |A^+B^+| \leq |A^+C^-| + |B^+C^+|$$

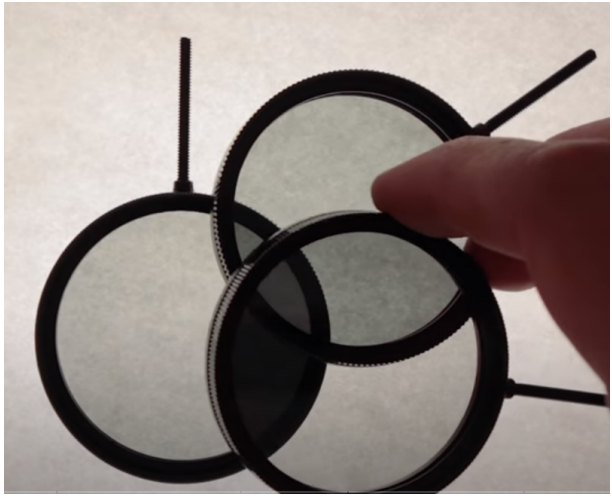
Ce qui, en termes de probabilités d'être dans un ensemble ou un autre revient à dire

$$P(A^+B^+) \leq P(A^+C^-) + P(B^+C^+)$$

On peut démontrer de la même manière d'autre inégalités, en particulier

$$P(A^+C^-) \leq P(A^+B^-) + P(B^+C^-)$$

Lumière polarisée



Mise en équations physiques 1/2

Considérons 3 polariseurs A, B et C dont les angles de polarisation sont α, β et γ.

Selon l'approche de la physique classique associée aux principes de localité, causalité et réalisme, il existe pour chaque photon des variables cachées qui indiquent si un photon va ou non traverser le polariseur A, B ou C s'il est placé sur la route du photons. Du point de vue ensembliste, la situation est analogue aux enfants qui portent ou non des écharpes, des bonnets et des lunettes que nous avons vue plus haut.

La probabilité de passer A et B est $P(A^+B^+) = cos^2(\alpha - \beta)$ et celle de passer A mais pas B est son complément donc $P(A^+C^-) = sin^2(\alpha - \beta)$.

Mise en équations physiques 2/2

On a l'inégalité ensembliste $P(A^+C^-) \leq P(A^+B^-) + P(B^+C^-)$, on en déduit

$$sin^2(\alpha - \gamma) \leq sin^2(\alpha - \gamma) + sin^2(\alpha - \beta)$$

Si on prend $\alpha = 0, \beta = \pi/8, \gamma = \pi/4$, on obtient

- $sin^2(\alpha - \gamma) = sin^2(\pi/4) = 1/2$
- $sin^2(\alpha - \beta) = sin^2(\pi/8) = \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.15 < 0.16$
- $sin^2(\beta - \gamma) = sin^2(\pi/8) = \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.15 < 0.16$

Si on rapporte dans l'équation enqsembliste, on obtient le résultat absurde $0.5 < 0.32$!

Il y a une contradiction notable.

Plan

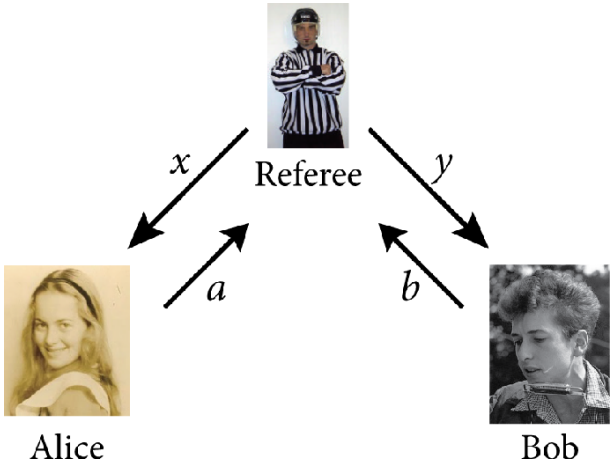
28 Un petit détour par la théorie de la complexité
29 Zoologie de Karp des problèmes NPC
30 Éléments de physique et théorème adiabatique
31 Quelques problèmes classiques
32 QUBO et les autres problèmes NPC
33 Machine Pasqal et problème MIS
34 VQE
35 QAOA
36 Inégalités de Bell
37 Le jeu CHSH

Les règles du jeu CHSH

Le jeu CHSH doit son nom a ses creéateurs, John Clauser, Michael Horne, Abner Shimony, et Richard Holt. C'est une expérience de pensée dans lequel deux opérateurs, Alice (A) et Bob (B) sont éloignés d'une grande distance, si grande qu'il leur est impossible de communiquer dans le temps du jeu. Par exemple, Alice est sur Terre, tandis que Bob est sur Mars, à au moins trente minutes-mulière de là.

Un arbitre, que l'on désignera comme Charlie (C), choisit deux bits x et y, $x, y \in \{0; 1\}$. En réponse, Alice et Bob utilise, sans pouvoir communiquer pendant le jeu, une stratégie qui leur permet de produire deux bits a et b, $a, b \in \{0; 1\}$.

CHSH



CHSH sous forme mathématique

Si l'équation suivante est remplie, alors Alice et Bob gagnent le jeu

$$x \wedge y = a \oplus b$$

Le ET logique entre x et y doit être égale au XOR entre a et b, ce qui revient à écrire, en arithmétique modulo 2

$$x.y \equiv a + b \ [2]$$

Avec une approche classique, on peut démontrer, avec ou sans secret partagé, **qu'il n'est pas possible de gagner le jeu CHSH avec plus de 75% de chances**.

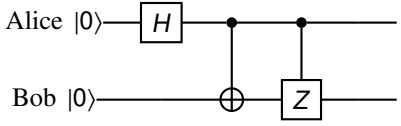
CHSH en approche quantique

Dans cette implémentation, on utilise une paire intriquée, dont Alice et Bob possède chacun un qubit

On réalise un système intriqué défni par

$$|A, B\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

par exemple on peut le construire avec un circuit quantique comme celui-ci



Alice et Bob prépare, avant le jeu CHSH, des paires intriqués, et chacun emporte avec lui un qubit de la paire.

CHSH : stratégie quantique

Soit $R(\theta$ la rotation dans $\mathbb{C}^4$ définie par

$$R(\theta) = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$$

La stratégie de Alice est Bob est alors la suivante

- Alice applique une rotation $R(\theta_A)$ avec $\theta_A = \frac{(4x-1)\pi}{16}$, c'est à dire $-\pi/16$ si $x = 0$ et $3\pi/16$ si $x = 1$
- Bob applique de son côté une rotation de $\theta_B = \frac{(4y-1)\pi}{16}$
- Alice et Bob mesure leurs qubits respectifs dans la base $(|0\rangle, |1\rangle)$

Mathématiquement cela revient à dire qu'Alice applique $R(\theta_A) \otimes I$ tandis que Bob applique $I \otimes R(\theta_B)$. Ces deux opérations commuttent, le résultat sur $|A, B\rangle$ est donc

$$(R(\theta_A) \otimes I) \times (I \otimes R(\theta_B)) |A, B\rangle = (R(\theta_A) \otimes R(\theta_B) |A, B\rangle .$$

Développons le calcul 1/2

$$\begin{pmatrix} cos(\theta_A).\begin{pmatrix} cos(\theta_B) & -sin(\theta_B) \\ sin(\theta_B) & cos(\theta_B) \end{pmatrix} & -sin(\theta_A).\begin{pmatrix} cos(\theta_B) & -sin(\theta_B) \\ sin(\theta_B) & cos(\theta_B) \end{pmatrix} \\ sin(\theta_A).\begin{pmatrix} cos(\theta_B) & -sin(\theta_B) \\ sin(\theta_B) & cos(\theta_B) \end{pmatrix} & cos(\theta_A).\begin{pmatrix} cos(\theta_B) & -sin(\theta_B) \\ sin(\theta_B) & cos(\theta_B) \end{pmatrix} \end{pmatrix} . \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

Développons le calcul 2/2

$$
\begin{aligned}
(R(\theta_A) \otimes R(\theta_B)\,|A,B\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} cos(\theta_A)cos(\theta_B) - sin(\theta_A)sin(\theta_B) \\ cos(\theta_A)sin(\theta_B) + sin(\theta_A)cos(\theta_B) \\ sin(\theta_A)cos(\theta_B) + cos(\theta_A)sin(\theta_B) \\ sin(\theta_A)sin(\theta_B) - cos(\theta_A)cos(\theta_B) \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} cos(\theta_A + \theta_B) \\ sin(\theta_A + \theta_B) \\ sin(\theta_A + \theta_B) \\ -cos(\theta_A + \theta_B) \end{pmatrix} \\
&= \frac{1}{\sqrt{2}}(cos(\theta_A + \theta_B)\,|00\rangle + sin(\theta_A + \theta_B)\,|01\rangle \\
&+ sin(\theta_A + \theta_B)\,|10\rangle + cos(\theta_A + \theta_B)\,|11\rangle) \\
&= \frac{1}{\sqrt{2}} cos(\theta_A + \theta_B)(|00\rangle - |11\rangle) + \frac{1}{\sqrt{2}} sin(\theta_A + \theta_B)(|01\rangle + |10\rangle)
\end{aligned}
$$

Discussion

Discutons ce résultat pour obtenir la probabilité de gagner donc d'avoir $a \oplus b = x_l andy$.

On notera que l'on a

$$\theta_A + \theta_B = \frac{(4x-1)\pi}{16} + \frac{(4y-1)\pi}{16} = \frac{(4(x+y)-2)\pi}{16} = \frac{(2(x+y)-1)\pi}{8}$$

349 / 370

Différents cas 1/2

Si $x = y = 0$, alors $a \oplus b = 0$, ce qui revient à mesurer soit $|00\rangle$ soit $|11\rangle$. Ces deux vecteurs ont l'amplitude complexe $\frac{1}{\sqrt{2}} cos(\theta_A + \theta_B)$, donc on une probabilité de mesure égale à $\frac{1}{2} cos^2(\theta_A + \theta_B)$ pour chacun. La probabilité de vooir l'un ou l'autre est donc

$$P_{00} = 2.\frac{1}{2} cos^2(\theta_A + \theta_B) = cos^2(\theta_A + \theta_B)$$

Dans ce cas, $\theta_A + \theta_B = \frac{(2(x+y)-1)\pi}{8} = -\frac{\pi}{8}$ donc $P_{00} = cos^2(\pi/8)$

Si $x = 0, y = 1$ ou $x = 1, y = 0$, alors $a \oplus b = 0$, on s'intéresse encore à $|00\rangle$ et $|11\rangle$ qui ont chacun la probabilité $\frac{1}{2} cos^2(\theta_A + \theta_B)$ d'être mesurés.
Dans ce cas de figure $\theta_A + \theta_B = \frac{(2(x+y)-1)\pi}{8} = \frac{\pi}{8}$ donc $P_{01} = P_{10} = 2.\frac{1}{2} cos^2(\pi/8) = cos^2(\pi/8$

Différents cas 1/2

Si $x = y = 1$ alors $a \oplus b = 1$ donc a et b sont différents et on va s'intéresser à $|01\rangle$ et $|10\rangle$.
Chacun dispose d'une amplitude $\frac{1}{\sqrt{2}} sin(\theta_A + \theta_B)$, soit une probabilité de mesure égale à $\frac{1}{2} sin^2(\theta_A + \theta_B)$.
Dans ce cas de figure $\theta_A + \theta_B = \frac{(2(x+y)-1)\pi}{8} = \frac{3\pi}{8}$
On remarque que $3\pi/8$ et $\pi/8$ sont symétrique par raport à $\pi/4$, par conséquent $sin(3\pi/8) = cos(\pi/8)$. Par conséquent $P_{11} = 2.\frac{1}{2} sin^2(\theta_A + \theta_B) = sin^2(3\pi/8) = cos^2((\pi/8))$

Conclusion

On constate que les probabilités P_{xy} de gagner pour chaque cas valent toutes $cos^2(\pi/8)$. Or, la trigonométrie permet d'établir que

$$cos^2(\pi/8) = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.853553391 \approx 85.35\%$$

La stratégie quantique, basée sur le partage d'une paire intriquée permet de remporter le jeu CHSH avec une pprobabilité supérieure à 85%, bien supérieure aux 75% que permet l'approche classique.

Plan

38 Programmation dans l'environnement QLM

39 Programmation dans l'environnement Pulser de PASQAL

Plan

38 Programmation dans l'environnement QLM

39 Programmation dans l'environnement Pulser de PASQAL

Programmation avec Pulser - les grandes lignes

Les machines PASQAL se programment à l'aide de l'environnement Pulser en Python.

Un programme Pulser est avant tout "une expérience de physique quantique instrumentée".

- importance du phénomène de *blocage de Rydberg*
- une centaine d'atomes utilisables dans la version livrée au CEA, sur une structure plane

Fondamentalement, les machines PASQAL ne savent résoudre qu'un seul type de problème :le problème MIS sur un graphe unitaire.

Il faut d'abord convertir son problème cible en problème MIS et savoir convertir l'état final mesuré en solution.

Concepts mathématiques - théorie des graphes

Le problème que peut traiter la machine est PASQAL est le *Maximum Independant Set*

- considérons un graphe $(G; E)$
  - G est un ensemble de points, ou sommets (ou *vertices*) dans un espace à n dimensions
  - E est un ensemble de segments, ou arêtes (ou *edges*) qui relient deux points de G
- on cherche le, ou les, plus grand(s) ensemble de sommets dont les membres ne sont pas connectés entre eux.

Dans le cas des machines PASQAL, on considère des graphes **unitaires**

- les sommets dont la distance est inférieur à un rayon **R** donné sont connectés
- deux sommets connectés sont forcément plus proche que **R**

Le problème MIS est dual du problème MCS (*Minimum Convering set*

- identifier l'ensemble le plus petit possible de sommets où poser des "caméras" pour voir toutes les arêtes du graphe
- on démontre facilement que les solutions de MIS et MVS sont complémentaire

Les bases physiques

Pour résoudre MIS, la machine PASQAL met en oeuvre différents mécanismes

- des atomes de rubidium monovalents émis par une ampoule dans une chambre à vides, ralentis et positionnés par des lasers
- le niveau de valence le plus bas et le niveau le plus haut encode les états $|0\rangle$ et $|1\rangle$
- les atomes sont intriqués via le phénomène de blocage de Rydberg (*Rydberg blocade*)
- on sait éjecter les atomes dans l'état $|1\rangle$ (mais on sait parfaitement où ils étaient)
- on sait voir les autres par flurorescence, on sait donc mmesurer les états de chaque atome

Par ailleurs

- ne sont intricables que des atomes dont la distance est inférieur au rayon de Rydberg
- deux atomes intriqués sont dans l'état $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Utilisation de lasers

La machine PASQAL utilise les lasers pour deux propos

- ralentir et positionner les atomes de rubidium émis par l'ampoule
- faire sortir les atomes de l'état $|0\rangle$ et déclencher des blocages de Rydberg

L'hamiltonien qui correspond au système est formellement très proche de la formulation du problème de Ising.

Programmation Pulser

La programmation avec le framework Pulser en Python est assez simple

- On calcule le rayon de Rydberg
- on place les atomes pour qu'ils soient les sommets d'un graphe uniaire dont le rayon correspond au rayon de Rydberg
- on décrit la forme d'une émission laser globale qui va éclairer tous les atomes et initier des blocages de Rydberg
- tire les lasers à plusieurs reprises
- on réalise les mesures pour faire ressortir les états les plus probables finals

Exemple de code - Initialisation

On initialise l'environnement de programmation comme suit

```
import numpy as np
from pulser import Pulse, Sequence, Register
from pulser_simulation import Simulation
from pulser.devices import MockDevice
from pulser.waveforms import RampWaveform, ConstantWaveform

import matplotlib.pyplot as plt
import qutip
```

Exemple de code - description du graphe

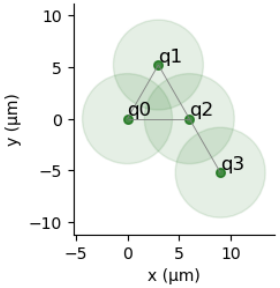
```
# Define a dictionary where each key is the name of the qubit,
# and each value is the qubit's position (in um)

qubit_positions = {
    'q0': (0, 0),
    'q1': (3, 5.2),
    'q2': (6, 0),
    'q3': (9, -5.2)
}
```

Ce dictionnaire est ensuite transformé en registre.

```
# Arrangements of qubits on the machine are called a register
# Define a register in Pulser by passing the qubit dictionary
reg = Register(qubit_positions)
reg.draw()
```

Rayon du graphe unitaire

```
# Define the maximum Rabi frequency via a blockade radius
blockade_radius = 8.7
Omega_max = MockDevice.rabi_from_blockade(blockade_radius)

# Visualize the edges induced by the chosen blockade radius
reg.draw(blockade_radius=blockade_radius)
```

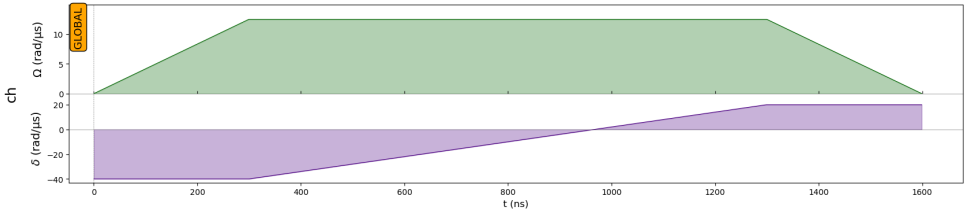


Définir l'impulsion laser

```
# A Sequence is the object that contains all
# the info about the quantum evolution
seq = Sequence(reg, MockDevice)

# Now we want to fill the channel with pulses
# First we need to define the waveforms for the pulses
# First ramp
omega_wf_1 = RampWaveform(300, 0, Omega_max)

#arguments are duration (ns), detuning (rad/us)
delta_wf_1 = ConstantWaveform(300, -40)

first_pulse = Pulse(omega_wf_1, delta_wf_1, 0)
seq.add(first_pulse, 'ch')
seq.draw()
```

Forme de l'impulsion

L'impulsion laser aura ainsi la forme suivante

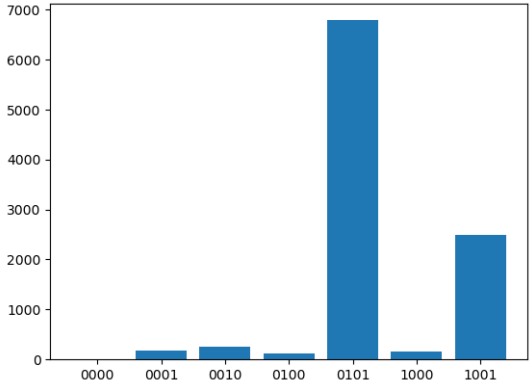


Pulser - fin du code

```
# The sequence is ready now for simulation

sim = Simulation(seq)
results = sim.run()

# The result can be sampled
samples = results.sample_final_state(10000)

# And the sampling can be visualized
plt.bar(samples.keys(), samples.values())
```

Résultat

On voit le résultat suivant



On voit deux solutions : $|0101\rangle$ et $|1001\rangle$. ce sont les solutions du problème MIS.

Les problèmes NP-Complets

Certains problèmes NP-Complets sont particulièrement d'un point de vue de l'informatique quantique

- le problème d'optimisation QUBO (voir slide suivant)
- le problème **MaxCut** (couper un graphe en deux ensembles complémentaires qui maximise les coupes des arêtes)
- le problème **Maximum Independant Set (MIS)** et son dual le problème **Maximum Vertices Conver (MVC)**
- les problèmes de coloration de graphes
- le problème et *SAT* et sa variante **3-SAT** (satisfaisabilité booléenne)
- le problème du voyageur de commerce (**Travelling Sales Person** (TSP)) et le problème du *cycle hamiltonien*
- les problèmes de détection de clique maximum
- le problème du sac à dos

Le problème QUBO

L'acronyme *QUBO* signifie *Quadratic Unconstrained Binary Optimisation*. Il permet de résoudre des problèmes d'optimisation qui se ramènent, à la recherche d'optima d'une forme quadratique.

L'énoncé de QUBO est le suivant : étant donné un entier $n \in \mathbb{N}$, étant donné $\mathbb{B}^n = \{0; 1\}n$, l'ensemble des vecteurs de taille n formés de 0 et de 1, étant donné une forme quadratique f_Q représentée par une matrice $Q \in \mathbb{R}^{n \times n}$, quel est la valeur $x^* \in \mathbb{B}^n$ qui minimise $f_Q(x) = x^T.Q.x$ D'une manière générale, on ajoute parfois au terme quadratique un terme linéaire, l'énoncé devient alors

$$Q \in \mathbb{R}^{n \times n}, c \in \mathbb{R}^n, \text{ trouver la valeur } x^* \text{ qui minime } f(x) = x^T.Q.x + c^T.x$$

MIS est NP-Complet

On peut prouver que MIS est NP-Complet

- il est représentatif de la classe de problème NP
- il ne peut être résolu classiquement en un temps polynomial (sauf si $P = NP$)

On peut souvent convertir un problème NPC en un autre NPC (par exemple résoudre MIS avec un QUBO).
Savoir résoudre MIS est donc très intéressant.

Fonctionnalités futures

Dans les prochaines versions de leur hardware, PASQAL sera capable

- de gérer plus d'atomes (quelques centaines)
- de disposer les atomes en 3 dimensions (actuellement on fait juste de la 2D)
- d'éclairer certains atomes différemment les uns des autres

Ce dernier point est important, il permet d'implémenter le problème *Weighted MIS (MWIS)* ou "MIS à poids".
La formulation MWIS est important : un problème en $O(N^6)$ en MIS devient $O(N^2)$ en MWIS.
Il est nécessaire de mettre en place beaucoup de middleware pour bien exploiter cette conversion.