Stage de L3

Elisa Rebolini

14 décembre 2010

Laboratoire d'accueil

Ce stage a été réalisé sous la direction du professeur Frédéric Magniez qui travaille au sein de l'équipe algo et du groupe quantique. Je fus très bien accueillie malgré les déplacements successifs de Frédéric. Mon stage s'est donc étalé de début juin à mi juillet et continua début septembre.

Introduction

Selon la loi de Moore, les composants des ordinateurs devraient atteindre la taille de l'atome dans les années 2020. A cette échelle, des phénomènes quantiques entrent en jeu. Le fonctionnement de composants électroniques serait donc fortement pertubé. Depuis les années 90, est apparu le concept d'ordinateur quantique, calculateur reposant sur les propriétés quantiques de la matière. Alors que les physiciens tentent de mettre au point un tel ordinateur, les informaticiens se sont penchés sur ses capacités et ont développés un certain nombre d'algorithmes, dits quantiques, utilisant ces propriétés. Dans certains cas, ces algorithmes sont nettement plus puissants que leurs équivalents classiques. On peut notamment citer l'algorithme de Shor [1] qui permet de décomposer les grands nombres en facteurs premiers qui apporte une amélioration exponentielle par rapport aux algorithmes classiques et l'algorithme de Grover [2] qui permet de faire une recherche dans une base de données non triée. On s'intéressera dans la suite plus particulièrement à l'algorithme de Grover. L'algorithme initial fut réalisé en 1996 par Lov Grover et permet d'obtenir une amélioration quadratique de la complexité par rapport aux algorithmes classiques. Plusieurs versions furent proposées depuis, comme par exemple, par évolution adiabatique [3] ou par mesure [4]. La version adiabatique de l'algorithme de Grover fait intervenir le théorème adiabatique. Bien qu'il soit prouvé dans le cadre de Grover, les hypothèses de ce théorème restent mal connues et la preuve incomplète. La version par mesure de l'algorithme permet de se passer de ce théorème.

1 Le problème de Grover

Le problème de Grover consiste à chercher un élément particulier dans une base de données sans structure. Par exemple, on cherche dans un annuaire téléphonique à qui appartient le numéro 0168954231.

Définition :

Données :
Soient un ensemble $DB = [0, 1, ..., N-1]$ et une fonction $C : DB \mapsto \{0, 1\}$ tels que $\exists! m \in DB, C(m) = 1$ et $C(i) = 0$ si $i \neq m$
Problème :
Trouver $i \in DB$ tel que $C(i) = 1$

2 Quelques notions de quantique

2.1 Evolution

Alors qu'en physique classique, un système est défini par un certain nombre de grandeurs (vitesse, position...) qui satisfont les lois de Newton, etc, un système quantique est entièrement défini par sa fonction d'onde $\psi(\overrightarrow{r}, \overrightarrow{p}, t)$ aussi notée, en notation de Dirac, $|\psi(t)\rangle$. Lorsque ce système est isolé, alors son évolution est déterminée par l'équation de Schrödinger

$$i\hbar \frac{\partial |\psi(t)\rangle}{\partial t} = H(t)|\psi(t)\rangle$$

où h est la constante de Planck, dans la suite, on prendra $\hbar = 1$, et où $H(t)$ est l'hamiltonien du système.

Un hamiltonien est un opérateur hermitien (auto-adjoint) qui décrit l'environnement dans lequel évolue le système quantique (champ magnétique, pesanteur, forces d'interactions entre les particules).

Lorsque l'Hamiltonien ne dépend pas du temps, l'équation de Schrödinger, peut se réécrire sous la forme d'une équation aux valeurs propres :

$$H|\psi_a(t)\rangle = E_a|\psi_a(t)\rangle$$

où les $|\psi_a(t)\rangle$ sont vecteurs propres de l'hamiltonien, associés aux valeurs propres E_a qui représentent l'énergie du système. Un état du système est alors une superposition d'états propres :

$$|\psi(t)\rangle = \sum_a \alpha_a |\psi_a(t)\rangle$$

On associe alors à l'hamiltonien, un opérateur unitaire :

$$U(t) = e^{-itH}$$

En développant H dans sa base propre, on a :

$$H = \sum_a E_a |E_a\rangle\langle E_a|$$

Dans le cas général, il peut exister une infinité de valeurs propres, cependant, dans la suite, on considérera qu'il en existe un nombre fini N. Physiquement, cette approximation est justifiée car la probabilité qu'un niveau d'énergie soit peuplé est inversement proportionnelle à son énergie. Les niveaux élevés peuvent donc être négligés. On écrira donc

$$|\psi(t)\rangle = \sum_{a=0}^{N-1} \alpha_a |\psi_a(t)\rangle$$

2.2 Mesure directe

Lorsque l'on effectue une mesure sur un système quantique, le système n'est plus isolé, son évolution n'est donc plus régie par l'équation de Schrödinger. Soit un système dans l'état $\psi = \sum_a \alpha_a |E_a\rangle$. Lors d'une mesure, on observe E_a avec probabilité $|\alpha_a|^2$ et le système se trouve alors dans l'état pur $|E_a\rangle$

2.3 Mesure par pointeur

Définition : pointeur

Un pointeur est un système auxiliaire que l'on met en interaction avec le système étudié afin de pouvoir réaliser des mesures indirectes. Dans la suite, on utilisera comme pointeur une particule libre à r états $|0\rangle$ et $|1\rangle$, d'hamiltonien P.

Mesure du pointeur

Considérons un pointeur dont la position est codée sur un qubit (ce que l'on utilisera par la suite) l'état du pointeur est donc une superposition $a|0\rangle + b|1\rangle$. Lorsque l'on mesure la position du pointeur, on obtient donc 0 avec probabilité $|a|^2$ et 1 avec probabilité $|b|^2$

Application : couplage

Lorsque l'on met le système en interaction avec le pointeur, l'Hamiltonien d'interaction est $H_{tot} \simeq H \otimes P$. L'opérateur unitaire s'écrit donc :

$$U(t) = \sum_a |E_a\rangle\langle E_a| \otimes e^{-itE_a P}$$

On prépare le pointeur dans l'état $|0\rangle$. La base de calcul de pointeur $\mathcal{B}_z = \{|0\rangle_z, |1\rangle_z\}$ est la base propre de P. Dans cette base, la représentation digitale de P est :

$$P = 1 - \sigma_z$$

où σ_z est l'opérateur z de Pauli dont la représentation matricielle est

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

On normalise P de sorte que :

$$P|z\rangle_z = \frac{z}{2}|z\rangle_z$$

Dans la base $\mathcal{B}_z$, l'état initial du pointeur s'écrit

$$|0\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle_z + |1\rangle_z\right)$$

Théorème

Soit un système dans l'état initial $|\psi\rangle = \sum_a \alpha_a |E_a\rangle$ avec $\alpha_0 \leq \frac{1}{\sqrt{2}}$ et un pointeur dans son état initial $|0\rangle_x$.

Après couplage pendant un temps t aléatoire dans l'intervalle $[1, 2...T]$ avec $T \geq T_m = \dfrac{10^3}{2}\sum_{a\neq 0} \dfrac{\alpha_a^2}{\sin\dfrac{E_a}{4}}$, et après mesure du pointeur on obtient 0 avec une probabilité supérieure à $\dfrac{3\alpha_0^2 - 1}{2} \pm 10^{-3}$.

On est alors dans l'état $|\psi_0\rangle$ tel que $|\langle E_0|\psi_0\rangle|^2 \geq \dfrac{4}{3}\alpha_0^2$ avec probabilité supérieure à $\frac{2}{3}$

Preuve

Le système est dans l'état $|\psi\rangle = \sum_a \alpha_a |E_a\rangle$. On applique l'opérateur d'évolution pendant un temps t. On a alors :

$$U(t)\left(|\psi\rangle \otimes |0\rangle_x\right) = \sum_a \alpha_a |E_a\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_z + \exp\left(-\frac{itE_a}{2}\right)|1\rangle_z\right)$$

Par transformée de Fourier quantique, on a

$$\begin{aligned} U(t)(|\psi\rangle \otimes |0\rangle_x) &= \sum_a \alpha_a |E_a\rangle \otimes \left(\frac{1}{2}\left(1 + \exp\left(\frac{-itE_a}{2}\right)|0\rangle_x + \frac{1}{2}\left(1 - \exp(\frac{-itE_a}{2}\right)|1\rangle_x\right)\right) \\ &= \sum_a \alpha_a |E_a\rangle \otimes \exp\left(\frac{-itE_a}{4}\right)\left(\cos\left(\frac{tE_a}{4}\right)|0\rangle_x + i\sin(\frac{tE_a}{4})|1\rangle_x\right) \\ &= \sum_a \alpha_a \exp\left(\frac{-itE_a}{4}\right)\cos\left(\frac{tE_a}{4}\right)|E_a\rangle \otimes |0\rangle_x \\ &\quad + \sum_a i\alpha_a \exp\left(\frac{-itE_a}{4}\right)\sin\left(\frac{tE_a}{4}\right)|E_a\rangle \otimes |1\rangle_x \end{aligned}$$

Lorsqu'on effectue une mesure sur le pointeur, la probabilité d'observer l'état $|0\rangle_x$ est

$$p_0 = \sum_a \alpha_a^2 \cos^2\left(\frac{tE_a}{4}\right)$$

On pose $\theta_a = \dfrac{E_a}{2}$. On suppose l'énergie bornée par 1. Pour $t \in]0, T]$, l'espérance de p_0 est :

$$\begin{aligned}
E(p_0) &= \sum_{t=1}^{T} \frac{1}{T} \sum_a \alpha_a^2 \cos^2\left(\frac{t\theta_a}{2}\right) \\
&= \alpha_0^2 + \sum_{t=1}^{T} \frac{1}{T} \sum_{a\neq 0} \alpha_a^2 \cos^2\left(\frac{t\theta_a}{2}\right) \\
&= \alpha_0^2 + \frac{1}{2T} \sum_{t=1}^{T} \sum_{a\neq 0} \alpha_a^2 (\cos t\theta_a - 1) \\
&= \alpha_0^2 - \frac{1}{2} \sum_{a\neq 0} \alpha_a^2 + \frac{1}{2T} \sum_{a\neq 0} \alpha_a^2 Re\left(\sum_{t=1}^{T} \exp it\theta_a\right) \\
&= \alpha_0^2 - \frac{1}{2}(1-\alpha_0^2) + \frac{1}{2T} \sum_{a\neq 0} \alpha_a^2 Re\left(\exp i\theta_a \frac{\exp iT\theta_a - 1}{\exp i\theta_a - 1}\right) \\
&= \frac{3\alpha_0^2 - 1}{2} + \frac{1}{2T} \sum_{a\neq 0} \alpha_a^2 Re\left(\exp\frac{i\theta_a}{2} \exp\frac{iT\theta_a}{2}\right) \frac{\sin\dfrac{T\theta_a}{2}}{\sin\dfrac{\theta_a}{2}} \\
&= \frac{3\alpha_0^2 - 1}{2} + \frac{1}{2T} \sum_{a\neq 0} \alpha_a^2 \cos\left(\frac{\theta_a(T+1)}{2}\right) \frac{\sin\dfrac{T\theta_a}{2}}{\sin\dfrac{\theta_a}{2}}
\end{aligned}$$

$$\begin{aligned}
\left|E(p_0) - \frac{3\alpha_0^2 - 1}{2}\right| &= \left|\frac{1}{2T} \sum_{a\neq 0} \alpha_a^2 \cos\left(\frac{\theta_a(T+1)}{2}\right) \frac{\sin\dfrac{T\theta_a}{2}}{\sin\dfrac{\theta_a}{2}}\right| \\
&\leq \left|\frac{1}{2T} \sum_{a\neq 0} \frac{\alpha_a^2}{\sin\dfrac{\theta_a}{2}}\right| \\
&\leq \left|\frac{1}{2T} \sum_{a\neq 0} \frac{\alpha_a^2}{\sin\dfrac{E_a}{4}}\right|
\end{aligned}$$

On pose $T_m = \dfrac{10^3}{2} \sum_{a\neq 0} \dfrac{\alpha_a^2}{\sin\dfrac{E_a}{4}}$

Par conséquent,

$$\boxed{\text{si } T \geq T_m \text{ alors } E(p_0) = \frac{3\alpha_0^2 - 1}{2} \pm 10^{-3}}$$

L'inégalité de Markov énonce que : $\mathbb{P}(X \geq \gamma) \leq \dfrac{1}{\gamma} E(X)$

Or $\mathbb{P}(p_0 \leq \gamma) \geq a \Leftrightarrow \mathbb{P}(p_0 \geq \gamma) \leq 1 - a = \frac{1}{\gamma}E(p_0)$

Donc $\mathbb{P}(p_0 \leq \gamma) \geq 1 - \frac{1}{\gamma}E(p_0)$

Comme $\alpha_0 \leq \frac{1}{\sqrt{2}}$, $E(p_0) \leq \frac{1}{4} \pm 10^{-3}$ pour $T \geq T_m$

D'après l'inégalité de Markov, on a $\mathbb{P}(p_0 \leq 3/4) \geq 2/3$

Après la mesure, on se trouve alors dans l'état

$$|\psi_0\rangle = \frac{1}{\sum_a \alpha_a^2 \cos^2\left(\frac{tE_a}{4}\right)} \sum_a \alpha_a \exp\left(\frac{-itE_a}{4}\right) \cos\left(\frac{tE_a}{4}\right) |E_a\rangle$$

$$|\langle E_0|\psi_0\rangle|^2 = \frac{\alpha_0^2}{\sum_a \alpha_a^2 \cos^2\left(\frac{tE_a}{4}\right)} = \frac{\alpha_0^2}{p_0}$$

On a donc avec probabilité supérieure à $\frac{2}{3}$ que $\|\langle E_0\|\psi_0\rangle\|^2 \geq \frac{4}{3}\alpha_0^2$

3 Grover par mesure

Soit $\mathcal{H}$ un espace de Hilbert de dimension N, on note $|i\rangle$ ses vecteurs de base avec $i = 0, ..., N-1$

On note H_B l'hamiltonien de base, dont l'état fondamental est la superposition uniforme. On note H_P l'hamiltonien du problème dont l'état fondamental est la solution du problème de Grover étudié ici, ie, $H_P. = Id - |m\rangle\langle m|$ On pose $H(s) = sH_P + (1-s)H_B$. En particulier $H(\frac{1}{2}) = \sum_a E_a |E_a\rangle\langle E_a|$

Etat de l'art : Pour éviter d'utiliser le théorème adiabatique, Farhi et al. proposent un algorithme par mesure qui consiste à faire évoluer le système entre l'état fondamental de H_B et celui de H_P en mesurant H pour $s = 1/M, 2/M ... 1$ où M est de l'ordre de $\sqrt{(N)}$. $H(s)$ et $H(s+1/M)$ étant très proches, lorsqu'on mesure $H(s+1/M)$ on obtient son fondamental avec une très grande probabilité.

Ici, on propose un autre algorithme par mesure où l'on ne fait que 2 mesures.

```
GROVER =
Créer une superposition uniforme
  |ψ⟩ = 1/√N Σ_{i=0}^{N-1} |i⟩
Appliquer H(1/2)
Réaliser une mesure par pointeur
  si 1
  alors abort
  sinon faire une mesure directe
```

On obtient alors l'élément recherché avec probabilité constante

Lemme

Soient $|E_0\rangle = \alpha_m|m\rangle + \sum_{i\neq m}\alpha_i|i\rangle$ et $|\psi_0\rangle = a|E_0\rangle + b|\chi\rangle$ tel que $\langle\chi|E_0\rangle = 0$ alors

$$|\langle m|\psi_0\rangle|^2 \geq \frac{1}{4}(|a|^2 + |\alpha_m|^2 - 1)^2$$

Preuve

$\langle m|\psi_0\rangle = a\alpha_m + b\langle m|\chi\rangle$
On pose $\langle m|\chi\rangle = \beta_m$ donc $\langle m|\psi_0\rangle = a\alpha_m + b\beta_m$
$|\langle m|\psi_0\rangle|^2 = |a\alpha_m + b\beta_m|^2$
Par normalisation, on a $|a|^2 + |b|^2 = 1$.

$$\begin{aligned}
|\langle m|\psi_0\rangle|^2 &= |a\alpha_m + b\beta_m|^2 \\
&\geq (|a\alpha_m| - |b\beta_m|)^2 \\
&\geq \left(\frac{|a\alpha_m|^2 - |b\beta_m|^2}{|a\alpha_m| + |b\beta_m|}\right)^2 \\
&\geq \frac{1}{4}(|a\alpha_m|^2 - |b\beta_m|^2)^2 \text{ car } |a\alpha_m| + |b\beta_m| \leq 2 \\
&\geq \frac{1}{4}\left(|a\alpha_m|^2 - (1-|a|^2)(1-|\alpha_m|^2)\right)^2 \\
&\geq \frac{1}{4}(|a|^2 + |\alpha_m|^2 - 1)^2
\end{aligned}$$

Preuve de l'algorithme

Le système est initialement dans l'état $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle$. Dans la base de l'hamiltonien $H(\frac{1}{2})$, cet état se réécrit $|\psi\rangle = \sum_a \alpha_a|E_a\rangle$ avec $\alpha_0 = \frac{1}{\sqrt{2}}$. D'après le théorème précédent, après mesure par pointeur on obtient 0 avec probabilité $\frac{1}{4} \pm 10^{-3}$ On est alors dans l'état $|\psi_0\rangle$ tel que $|\langle\psi_0|E_0\rangle|^2 \geq 2/3$ avec probabilité supérieure à $2/3$ et tel que $|\langle m|E_0\rangle|^2 = 1/2$ D'après le lemme, on a : $|\langle m|\psi_0\rangle|^2 \geq 1/144$

Conclusion

De nombreux algorithmes quantiques reposent sur le théorème adiabatique. Cependant, il a été prouvé que ce théorème est faux dans certaines conditions. Des alternatives à ce théorème sont donc développées, comme par exemple l'utilisation de la mesure directe et par pointeur. Au cours de ce stage, j'ai redécouvert des notions fondamentales de physique quantiques, découvert les différentes versions de l'algorithme de Grover et j'ai proposé une alternative au théorème adiabatique pour l'algorithme de Grover grâce à deux mesures successives. Ce résultat est prometteur et pourra peut être se généraliser à d'autres algorithmes

comme les marches quantiques. Je remercie chaleureusement Frédéric Magniez pour son encadrement, sa patience et son point de vue d'informaticien ! En tant que chimiste, j'abordais la question avec un point de vue très différent, et nos discussions furent donc très enrichissantes.

Références

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, 1997.

[2] Lov Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev.*, 1997.

[3] Jérémie Roland and Nicolas J. Cerf. Quantum search by local adiabatic evolution. *Phys. Rev.*, 2002.

[4] Andrew M. Childs, Enrico Deotto, Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Andrew J. Landahl. Quantum search by measurement. *Phys. Rev.*, 2002.