Calcul Quantique par Évolution Adiabatique

Lin Ke-Fong[*]

30 juillet 2002

Résumé : Le théorème adiabatique suggère un nouveau modèle de calcul quantique qui peut être simulé par un circuit quantique conventionnel de complexité polynomiale en temps et en espace. Cette méthode et son équivalence avec un circuit quantique sont décrites en détails dans ce rapport. Elle est appliquée sur un exemple : la recherche d'un élément marqué m parmis N éléments rangés sans ordre particulier (problème de Grover).

La contribution de ce rapport est d'expliciter la version quantitative du théorème adiabatique, de décrire en détail la méthode à utiliser pour créer des algorithmes de calcul adiabatique, de compléter la preuve de simulation par un circuit quantique conventionnel, et de vérifier les calculs pour l'application au problème de recherche.

1 Préliminaire

Pour commencer, il est utile de rappeler les postulats de la mécanique quantique qui serviront par la suite, ce sera l'occasion de donner quelques définitions et de préciser quelques hypothèses. Le premier tome de l'excellent ouvrage de Cohen-Tannoudji, Diu, et Laloë [1] contient les détails.

1.1 Un Premier Postulat

Soit un espace de Hilbert $\mathcal{H}$ de dimension N. Un *ket* $|\psi\rangle$ est un vecteur colonne, son vecteur dual $\langle\psi| = (|\psi\rangle)^\dagger$, aussi appelé *bra*, est le conjugué complexe de la transposé de $|\psi\rangle$, c'est un vecteur ligne. Le produit scalaire de deux kets $|u\rangle$ et $|v\rangle$ est donné par le produit $\langle u| \times |v\rangle$, aussi noté $\langle u|v\rangle$.

Postulat 1 *Soit $\mathcal{H}$ l'espace de Hilbert d'un système physique, à un instant t t donné, l'état du système est complètement défini par un vecteur d'état $|\psi(t)\rangle$.*

Une combinaison linéaire de vecteurs d'état est un vecteur d'état. Dans la suite, tous les vecteurs seront normés, c'est-à-dire que $\langle\psi(t)|\psi(t)\rangle = 1$.

1.2 Observable et Mesure

En mécanique classique, aucune différence n'est faite a priori entre la représentation mathématique d'une grandeur physique observable, par exemple la position ou la vitesse d'une particule, et les valeurs mesurées. Par contre en mécanique quantique, cette distinction est d'une importance fondamentale, elle permet entre autre d'expliquer le *principe d'incertitude d'Heisenberg*.

Postulat 2 *Toute grandeur physique mesurable $\mathcal{A}$ est décrite par un opérateur linéaire A sur $\mathcal{H}$, appelé observable, tel que : la mesure de $\mathcal{A}$ ne peut donner comme résultat qu'une des valeurs propres de l'observable A.*

Une *observable* A est un opérateur hermitien ($A = A^\dagger$) dont il est possible de former une base avec ses vecteurs propres, c'est toujours le cas lorsque $\mathcal{H}$ est de dimension finie. Soient a_k les valeurs propres de A. Une valeur propre a_k est *dégénérée* si sa multiplicité (son «degré de dégénérence») g_k est supérieur à 1, soit $|\psi_{k,i}\rangle$ avec $i \in [1, g_k]$ ses vecteurs propres normés, alors :

$$A\,|\psi_{k,i}\rangle = a_k\,|\psi_{k,i}\rangle\,.$$

[*]lin@lri.fr

Comme A est hermitien, les vecteurs propres $|\psi_{k,i}\rangle$ sont orthonormés : $\langle\psi_{k,i}|\psi_{l,j}\rangle = \delta_{kl}\delta_{ij}$. De plus, une mesure de $\mathcal{A}$ donnera toujours une valeur réelle car les valeurs propres sont réelles. Soit $\mathcal{E}_k$ le sous-espace propre de la valeur propre a_k. Dans le cas où a_k est non-dégénérée, $\mathcal{E}_k$ est généré par l'unique vecteur propre, dans le cas contraire, il est généré par les vecteurs propres $|\psi_{k,i}\rangle$ avec $i \in [1, g_k]$. Pour alléger les notations, $|\psi_k\rangle$ désignera toujours un vecteur normé de $\mathcal{E}_k$.

Postulat 3 *Une mesure de la grandeur physique $\mathcal{A}$ d'un système physique dans un état $|\psi(t)\rangle$ donnera la valeur propre a_k de l'observable A correspondante avec probabilité :*

$$\mathcal{P}(a_k) = \sum_{i=1}^{g_k} |\langle\psi_{k,i}|\psi(t)\rangle|^2.$$

Une mesure est donc un evenement de nature probabiliste. En définissant :

$$P_k = \sum_{i=1}^{g_k} |\psi_{k,i}\rangle\langle\psi_{k,i}|,$$

comme le projecteur orthogonal sur $\mathcal{E}_k$, il possible d'écrire :

$$\mathcal{P}(a_k) = \langle\psi(t)|P_k|\psi(t)\rangle .$$

Postulat 4 *Si la mesure de la grandeur physique $\mathcal{A}$ d'un système physique dans un état $|\psi(t)\rangle$ donne le résultat a_k, alors l'état immédiatement après la mesure est la projection normée de $|\psi(t)\rangle$ sur le sous-espace propre $\mathcal{E}_k$:*

$$\frac{P_k\,|\psi(t)\rangle}{\sqrt{\langle\psi(t)|P_k|\psi(t)\rangle}}.$$

L'état du système après une mesure est donc toujours un vecteur propre de A de valeur propre a_k.

Soient A et B deux observables possédant des vecteurs propres communs :

$$A\,|\psi_k\rangle = a_k\,|\psi_k\rangle \qquad \text{et} \qquad B\,|\psi_k\rangle = b_k\,|\psi_k\rangle\,,$$

ces deux observables sont alors dites *compatibles*, il est possible de mesurer simultanément les grandeurs physiques $\mathcal{A}$ et $\mathcal{B}$. Une condition nécessaire et suffisante est que A et B commutent : $AB - BA = 0$. Dans le cas contraire, il est impossible de mesurer en même temps ces deux quantités avec une précision arbitraire, c'est le principe d'incertitude. Il est par exemple impossible de connaître à la fois la position et la vitesse d'une particule.

1.3 Équation de Schrödinger et Évolution

Postulat 5 *Un système physique de vecteur d'état $|\psi(t)\rangle$ et* d'hamiltonien $H(t)$ *évolue dans le temps selon* l'équation de Schrödinger *:*

$$i\hbar\frac{d}{dt}\,|\psi(t)\rangle = H(t)\,|\psi(t)\rangle\,. \tag{1}$$

Exemple : Voici un petit exemple issu de la physique. Soit une particule de masse m se déplaçant sur l'axe des x avec une vitesse non-relativiste v, celle-ci est soumise à un champs de force $F(x,t)$, son énergie totale est :

$$E = \frac{p^2}{2m} + V(x,t) \qquad \text{avec } p = mv,$$

$p^2/2m$ est son énergie cinétique et $V(x,t)$ son énergie potentielle. Sa fonction d'onde est :

$$\psi(x,t) = Ce^{i(px-Et)/\hbar},$$

C est une constante et $\hbar = h/2\pi$, avec $h = 6,626 \times 10^{-34}$ J/s la constante de Planck. En dérivant cette fonction d'onde par rapport au temps, il vient :

$$\frac{\partial\psi(x,t)}{\partial t} = -\frac{iE}{\hbar}\psi(x,t),$$

en la dérivant deux fois par rapport à x, il vient :

$$\frac{\partial^2 \psi(x,t)}{\partial x^2} = -\frac{p^2}{\hbar^2}\psi(x,t),$$

ce qui permet d'aboutir à *l'équation de Schrödinger* :

$$i\hbar \frac{\partial \psi(x,t)}{\partial t} = \underbrace{\left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x,t)\right]}_{H(t)} \psi(x,t),$$

où $H(t)$ est *l'hamiltonien* de la particule. L'hamiltonien $H(t)$ d'un système physique est l'opérateur hermitien qui décrit complètement son évolution dans le temps. C'est l'observable correspondant aux différents d'états d'énergie du système. $\square$.

À tout instant t, les valeurs propres $E_k(t)$ et les vecteurs propres $|\psi_{k,i}(t)\rangle$ de $H(t)$ satisfont :

$$H(t)\,|\psi_{k,i}(t)\rangle = E_k(t)\,|\psi_{k,i}(t)\rangle\,, \tag{2}$$

un vecteur propre de $H(t)$ est aussi appelé *état propre*. Soit M le nombre de sous-espaces propres $\mathcal{E}_k$. Les valeurs propres seront supposées ordonnées par énergie croissante : $E_0(t) < E_1(t) < \cdots < E_{M-1}(t)$, ainsi $E_0(t)$ correspond à l'état *fondamental*, c'est-à-dire à l'état de plus basse énergie.

Définition 1 (Transformation unitaire) *L'évolution de t_0 à t de l'équation de Schrödinger selon l'hamiltonien $H(t)$* induit *une transformation unitaire $U(t)$ tel que :*

$$U(t)\,|\psi(t_0)\rangle = |\psi(t)\rangle\,. \tag{3}$$

En particulier, si les hamiltoniens $H(t_1)$ et $H(t_2)$ commutent pour tout t_1 et t_2, alors :

$$U(t) = \exp - \left(\frac{i}{\hbar}\int_{t_0}^{t} H(t')dt'\right).$$

Les portes quantiques correspondent à des transformations unitaires.

Dans le cas où l'hamiltonien H est indépendant du temps, il est possible d'obtenir une solution exacte à l'équation de Schrödinger, il suffit de la projeter sur les vecteurs propres $|\psi_{k,i}\rangle$:

$$i\hbar\frac{d}{dt}\langle\psi_{k,i}|\psi(t)\rangle = \langle\psi_{k,i}|H|\psi(t)\rangle\,.$$

Comme H est hermitien :

$$(H\,|\psi_{k,i}\rangle)^\dagger = \langle\psi_{k,i}|\,H = \langle\psi_{k,i}|\,E_k = (E_k\,|\psi_{k,i}\rangle)^\dagger,$$

en prenant $c_{k,i}(t) = \langle\psi_{k,i}|\psi(t)\rangle$, il est possible d'écrire :

$$i\hbar\frac{d}{dt}c_{k,i}(t) = E_k c_{k,i}(t),$$

en intégrant cette équation, il vient :

$$c_{k,i}(t) = c_{k,i}(t_0)\exp\left(-\frac{i}{\hbar}E_k(t-t_0)\right). \tag{4}$$

Dans le cas où l'hamiltonien $H(t)$ dépend du temps, il n'est en général pas possible de résoudre l'équation de Schrödinger de manière exacte, sauf dans des cas très simples. Néanmoins, il est possible de développer $|\psi(t)\rangle$ sur les vecteurs propres de $H(t)$, l'expression suivante sera utile pour la suite :

$$|\psi(t)\rangle = \sum_{k=0}^{M-1}\sum_{i=1}^{g_k} C_{k,i}(t)\,|\psi_{k,i}(t)\rangle \exp\left(-\frac{i}{\hbar}\int_{t_0}^{t}E_k(t')dt'\right), \tag{5}$$

les coefficients $C_{k,i}(t)$ sont arbitraires.

2 Le Théorème Adiabatique

Le théorème adiabatique décrit le comportement des solutions de l'équation de Schrödinger lorsque l'hamiltonien $H(t)$ évolue lentement par rapport au temps. De manière informelle, ce théorème dit que si le système physique est initialement dans un état propre $|\psi_k(0)\rangle$ de valeur propre $E_k(0)$, et que l'évolution est *adiabatique*, c'est-à-dire suffisament lente, alors l'état final du système sera proche d'un vecteur propre $|\psi_k(T)\rangle$ de valeur propre $E_k(T)$.

2.1 Énoncé du Théorème

Theorème 1 (Théorème adiabatique) *Soit T la durée de l'évolution. Soit le changement de variable : $s = t/T$. Soit un hamiltonien $H(s) = \sum_{k=0}^{M-1} E_k(s)P_k(s)$ défini pour la période $0 \le s \le 1$ tel que $e_i(s) \neq e_j(s)$ si $i \neq j$. Les projecteurs P_k sont supposés continus et dérivables deux fois. Soit $|\psi(s)\rangle$ le vecteur d'état du système. La transformation unitaire $U_T(s)$ est solution de l'équation de Schrödinger :*

$$i\hbar \frac{d}{ds} U_T(s) = TH(s)U_T(s)$$

alors:

$$\lim_{T\to+\infty} U_T(s)P_k(0)\,|\psi(0)\rangle = P_k(s) \lim_{T\to+\infty} U_T(s)\,|\psi(s)\rangle$$

pour tout k.

Le deuxième tome de l'ouvrage de Messiah [2] démontre ce théorème.

2.2 Un Énoncé Quantitatif

L'inconvénient du précédent théorème est qu'il n'est pas quantitatif, il ne donne aucune condition pour que l'évolution d'un système soit adiabatique, si ce n'est que celle-ci doit être suffisament lente. Il s'agit en fait de déterminer les conditions permettant de minimiser les probabilités de transitions *non-adiabatique* :

$$\mathcal{P}_{i\to f}(t) = |\,\langle\psi_f(t)|\psi(t)\rangle\,|^2,$$

où le système passe de l'état initial $|\psi_i(0)\rangle$ à un état final $|\psi_f(T)\rangle$ appartenant au sous-espace $\mathcal{E}_f(T)$ d'une valeur propre différente. Le théorème suivant, dont la preuve est inspirée de celle de Schiff [4], montre comment calculer ses probabilités, [2] et [3] proposent des preuves différentes.

Notation 1 *Soit un hamiltonien $H(t)$, soit $|\psi_i(t)\rangle$ et $|\psi_j(t)\rangle$ deux de ses vecteurs propres, et soit $M(t)$ un opérateur hermitien, alors :*

$$\langle M(t)\rangle_{i,j} = \langle\psi_i(t)|M(t)|\psi_j(t)\rangle\,.$$

Theorème 2 (Probabilité de transition non-adiabatique) *Soit un hamiltonien $H(t)$ défini pour $0 \le t \le T$ tel que $E_i(t) \neq E_k(t)$ si $k \neq i$. À l'état initial, le système est supposé être dans un état d'énergie $E_i(0)$, son vecteur d'état $|\psi(0)\rangle$ est donc un vecteur du sous-espace propre $\mathcal{E}_i(0)$. Soient une valeur propre $E_f(t)$ et un vecteur propre $|\psi_f(t)\rangle$ avec $f \neq i$, et soit un réel $\epsilon \le 1$, si l'inégalité suivante est vrai à tout instant t :*

$$\frac{\left|\left\langle \frac{\partial H(t)}{\partial t}\right\rangle_{f,i}\right|}{(E_f(t) - E_i(t))^2} \le \epsilon \tag{6}$$

alors la probabilité de transition non-adiabatique est :

$$\mathcal{P}_{i\to f}(T) \le \epsilon^2.$$

Preuve. Pour simplifier la preuve, les N valeurs propres seront supposées non dégénérées, et pour alléger les notations, la variable t sera omise, par exemple $E_k(t)$ sera écrit E_k. Comme il est d'usage en physique, $\dot{C}_k(t)$ correspondra à la dérivé par rapport au temps $dC_k(t)/dt$ de $C_k(t)$.

Une solution de l'équation de Schrödinger dont l'hamiltonien dépend du temps peut s'écrire sous la forme suivante :

$$|\psi(t)\rangle = \sum_{k=0}^{N-1} C_k(t)\, |\psi_k(t)\rangle \exp\left(-\frac{i}{\hbar}\int_0^t E_k(t')dt'\right).$$

En injectant cette expression dans l'équation de Schrödinger, il vient :

$$i\hbar \sum_{k=0}^{N-1} \left[\dot{C}_k\, |\psi_k\rangle + C_k\, |\frac{\partial \psi_k}{\partial t}\rangle - \frac{i}{\hbar} C_k\, |\psi_k\rangle\, E_k\right] \exp\left(-\frac{i}{\hbar}\int_0^t E_k(t')dt'\right)$$
$$= H(t) \sum_{n=0}^{N-1} C_k\, |\psi_k\rangle \exp\left(-\frac{i}{\hbar}\int_0^t E_k(t')dt'\right),$$

comme $H\,|\psi_k\rangle = E_k\,|\psi_k\rangle$, le dernier terme de gauche annule le terme de droite. En prenant le produit scalaire avec :

$$\langle \psi_f | \exp\left(\frac{i}{\hbar}\int_0^t E_f(t')dt'\right),$$

l'expression précédente devient :

$$\sum_{k=0}^{N-1} \dot{C}_k\, \langle \psi_f | \psi_k \rangle \exp\left(\frac{i}{\hbar}\int_0^t [E_f(t') - E_k(t')]dt'\right)$$
$$= -\sum_{k=0}^{N-1} C_k \left\langle \psi_f | \frac{\partial \psi_k}{\partial t} \right\rangle \exp\left(\frac{i}{\hbar}\int_0^t [E_f(t') - E_k(t')]dt'\right)$$

ce qui permet de conclure que :

$$\dot{C}_f = -\sum_{k=0}^{N-1} C_k \left\langle \psi_f | \frac{\partial \psi_k}{\partial t} \right\rangle \exp\left(\frac{i}{\hbar}\int_0^t [E_f(t') - E_k(t')]dt'\right). \tag{7}$$

En revenant à l'équation aux valeurs propres $H\,|\psi_k\rangle = E_k\,|\psi_k\rangle$, en la dérivant par rapport au temps, et en prenant le produit scalaire avec $\langle \psi_f |$, celle-ci devient :

$$\left\langle \psi_f \left| \frac{\partial H}{\partial t} \right| \psi_k \right\rangle + \left\langle \psi_f \, |H| \, \frac{\partial \psi_k}{\partial t} \right\rangle = \frac{\partial E_k}{\partial t} \langle \psi_f | \psi_k \rangle + E_k \left\langle \psi_f | \frac{\partial \psi_k}{\partial t} \right\rangle,$$

ce qui dans le cas où $f \neq k$ donne :

$$\left\langle \psi_f | \frac{\partial \psi_k}{\partial t} \right\rangle = \frac{\left\langle \frac{\partial H}{\partial t} \right\rangle_{f,n}}{E_k - E_f}.$$

Cela permet d'aboutir à l'expression finale :

$$\dot{C}_f(t) = -C_f(t) \left\langle \psi_f(t) | \frac{\partial \psi_f(t)}{\partial t} \right\rangle$$
$$- \sum_{k \in [0,N-1] \setminus \{f\}} \frac{C_k(t)}{E_k(t) - E_f(t)} \left\langle \frac{\partial H}{\partial t} \right\rangle_{f,k} \exp\left(\frac{i}{\hbar}\int_0^t [E_f(t') - E_k(t')]dt'\right). \tag{8}$$

Le carré du module de l'intégrale de $\dot{C}_f(t)$ correspond à la probabilité $\mathcal{P}_{i\to f}(t)$ d'obtenir l'état propre $|\psi_f(t)\rangle$ lors d'une mesure au temps t, c'est-à-dire la probabilité d'une transition non-adiabatique.

À présent, il s'agit d'essayer d'estimer $\mathcal{P}_{i\to f}(t)$. Si les quantités du côté droit de l'équation (8) sont supposées indépendantes du temps et que l'état initial du système est $|\psi_i(0)\rangle$, cette équation devient :

$$C_f(T) = \int_0^T \frac{1}{E_f - E_i} \left\langle \frac{\partial H}{\partial t} \right\rangle_{f,i} \exp\left(\frac{i}{\hbar}[E_f - E_i]t\right),$$

l'intégration se fait sans difficulté :

$$C_f(T) = -\frac{i\hbar}{(E_f - E_i)^2}\left\langle \frac{\partial H}{\partial t}\right\rangle_{f,i}\left[\exp\left(\frac{i}{\hbar}[E_f - E_i]T\right) - 1\right],$$

sont module au carré est :

$$\mathcal{P}_{i\to f}(T) = \frac{2\hbar^2}{(E_f - E_i)^4}\left|\left\langle \frac{\partial H}{\partial t}\right\rangle_{f,i}\right|^2\left[1 - \cos\left(\frac{[E_f - E_i]T}{\hbar}\right)\right].$$

Comme $1 - \cos(x) \leq 1$ pour tout x et que la constante $\hbar$ est minuscule, il est possible de conclure que si

$$\frac{\left|\left\langle \frac{\partial H(t)}{\partial t}\right\rangle_{f,i}\right|}{(E_f(t) - E_i(t))^2} \leq \epsilon$$

à tout instant t, alors :

$$\mathcal{P}_{i\to f}(T) \leq \epsilon^2.$$

Maintenant, dans le cas où les valeurs propres peuvent être dégénérées, la preuve est encore valable. La probabilité $\mathcal{P}_{i\to f}(T)$ est celle de passer d'un état propre du sous-espace $\mathcal{E}_i(0)$ à un état propre d'un autre sous-espace $\mathcal{E}_f(T)$ d'énergie différente. □

2.3 L'Énoncé Final

Pour majorer la probabilité d'une transition non-adiabatique d'un état propre de $\mathcal{E}_i$ vers un état propre d'énergie différent de $\mathcal{E}_f$ avec $f \in [0, M-1]\backslash\{i\}$, il faut majorer :

$$\frac{\left|\left\langle \frac{\partial H(t)}{\partial t}\right\rangle_{f,i}\right|}{(E_f(t) - E_i(t))^2},$$

cela se résume à majorer le numérateur et minorer le dénominateur. La minoration du dénominateur ne pose pas de problème, il suffit de prendre :

$$g(t) = \min_{f\in[0,M-1]\backslash\{i\}} (E_f(t) - E_i(t))^2, \tag{9}$$

à tout instant t. $g(t)$ est la fonction qui donne l'écart d'énergie minimum, le *gap* en anglais.

Définition 2 (Norme d'un vecteur) *Soit un ket $|x\rangle$, sa norme est ainsi définie :*

$$\||x\rangle\| = \sqrt{\langle x|x\rangle}. \tag{10}$$

Définition 3 (Norme d'un opérateur) *Soit M un opérateur hermitien, sa norme est définie ainsi:*

$$\|M\| = \max_{\||x\rangle\|=1} \|M\,|x\rangle\|. \tag{11}$$

En utilisant l'inégalité de Cauchy-Schwartz :

$$|\langle f|g\rangle|^2 \leq \langle f|f\rangle\langle g|g\rangle, \tag{12}$$

il est possible de majorer le numérateur :

$$\begin{aligned}\left|\left\langle \frac{\partial H(t)}{\partial t}\right\rangle_{f,i}\right| &\leq \||\psi_f(t)\rangle\| \cdot \left\|\frac{\partial H(t)}{\partial t}\,|\psi_i(t)\rangle\right\| \\ &\leq \left\|\frac{\partial H(t)}{\partial t}\right\|.\end{aligned}$$

Ce qui permet de conclure que pour un réel $\epsilon \leq 1$, si :

$$\frac{\|\partial H(t)/\partial t\|}{d(t)} \leq \epsilon \tag{13}$$

à tout instant t, alors :

$$\mathcal{P}_{i\to f}(T) \leq \epsilon^2$$

pour tout $f \in [0, M-1]\backslash\{i\}$. Pour connaître la probabilité totale de transition non-adiabatique, il suffit de sommer sur tous les vecteurs des $M-1$ sous-espaces propres $\mathcal{E}_f$.

Le théorème suivant est issu de l'article de van Dam, Mosca, et Vazirani [5]. Cet article ne donne aucune preuve, néanmoins l'auteur, après quelques efforts supplémentaires, semble avoir compris une chose finalement vraiment élémentaire.

Theorème 3 *Avec un changement de variable approprié, l'équation de Schrödinger devient :*

$$i\hbar\frac{d}{ds}\left|\psi(s)\right\rangle = \tau(s)H(s)\left|\psi(s)\right\rangle,$$

avec $\tau(s) = dt/ds$. Soit $g(s)$ la fonction donnant l'écart d'énergie minimum à chaque instant s. Pour que l'évolution soit adiabatique, il faut qu'à chaque instant s:

$$\tau(s) \geq \frac{\|\partial H(s)/\partial s\|}{\epsilon g^2(s)}. \tag{14}$$

Preuve. L'équation (13) montre comment majorer la probabilité d'une transition non-adiabatique, elle donne la condition «la plus sévère», toutes les autres probabilités de transition non-adiabatique sont plus faibles. L'équation (13) donne :

$$\frac{\|\partial H(t)/\partial t\|}{g(t)} \leq \epsilon,$$

en utilisant :

$$\left\|\frac{\partial H(t)}{\partial t}\right\| = \frac{ds}{dt}\left\|\frac{\partial H(s)}{\partial s}\right\|,$$

il vient :

$$\tau(s) = \frac{dt}{ds} \geq \frac{\|\partial H(s)/\partial s\|}{\epsilon g^2(s)}.$$

□

La suite du rapport utilisera la condition quantitative du théorème précédent.

3 Calcul par Évolution Adiabatique

Le théorème adiabatique suggère une nouveau modèle de calcul quantique. En effet, soit à minimiser une fonction $f(z) : \{0,1\}^n \to \mathbf{R}$, et soit un hamiltonien $H_1 = \sum_{z\in\{0,1\}^n} f(z)\left|z\right\rangle\!\left\langle z\right|$, l'état fondamental de H_1 code la valeur de z qui minimise $f(z)$, cet état est a priori inconnu. Soit un autre hamiltonien H_0 dont il est aisé de préparer l'état fondamental. Maintenant, s'il est facile de construire ces deux hamiltoniens et de préparer le système dans l'état fondamental de H_0 au temps initial, il est possible de résoudre ce problème de minimisation en faisant évoluer le système de l'hamiltonien H_0 à H_1 de manière adiabatique. L'évolution étant adiabatique, le système reste dans l'état fondamental, à la fin de ce processus, une mesure donne l'état fondamental de H_1 avec grande probabilité, ce qui permet d'obtenir la valeur z minimisant $f(z)$. Le théorème adiabatique impose un temps minimum nécessaire à l'évolution. Cette méthode a été proposée pour la première fois par Farhi, Goldstone, Gutmann, et Sipser [6], et analysée par van Dam, Mosca, et Vazirani [5].

3.1 Description de la Méthode

Méthode (Calcul Adiabatique) Soit à minimiser la fonction $f(z) : \{0,1\}^n \to \mathbf{R} \in O(n^d)$, et soit une fonction $h(z) : \{0,1\}^n \to \mathbf{R} \in O(n^{d'})$. Soient respectivement

$$H_0 = \sum_{z \in \{0,1\}^n} h(z) \, |\bar{z}\rangle\langle\bar{z}| \text{ et } H_1 = \sum_{z \in \{0,1\}^n} f(z) \, |z\rangle\langle z|$$

les hamiltoniens initial de base $|\bar{z}\rangle$ et final de base $|z\rangle$ du calcul adiabatique, $|\bar{z}\rangle = U\,|z\rangle$ pour un certain U fixé. Soit l'hamiltonien :

$$H(t) = (1 - s(t))H_0 + s(t)H_1,$$

avec $s(t)$ une fonction croissante continue et dérivable a priori quelconque tel que $s(0) = 0$ et $s(T) = 1$, $H(t)$ sera l'hamiltonien du système. La procédure est la suivante :

1. Le système est préparé dans l'état fondamental $|\psi_0(0)\rangle$ de l'hamiltonien de départ H_0.
2. Pendant un temps T, le système évolue suivant l'équation de Schrödinger avec l'hamiltonien $H(t)$, le théorème adiabatique fixe la durée T, celle-ci doit être suffisament longue pour que l'évolution soit adiabatique.
3. L'état final $|\psi(T)\rangle$ est mesuré, cette mesure est le résultat du calcul, elle donne avec grande probabilité $|\psi_0(T)\rangle$.

Pour que le théorème adiabatique puisse s'appliquer, il est nécessaire que pour tout $k \neq 0$, $E_0(t) \neq E_k(t)$ à chaque instant t, pour cela H_0 ne doit pas être diagonal dans la base de calcul $|z\rangle$, de cette manière H_0 et H_1 ne commutent pas.

3.2 Durée T de l'Évolution

En effectuant un changement de variable, il est possible d'écrire l'hamiltonien $H(t)$ sous la forme :

$$H(s) = (1 - s)H_0 + sH_1$$

pour $0 \leq s \leq 1$, avec entre autre $H(0) = H_0$ et $H(1) = H_1$. L'écart d'énergie minimum est celui entre l'état fondamental et le premier état d'excitation donc il s'agit de la fonction :

$$g(s) = E_1(s) - E_0(s).$$

Le théorème 3, celui énoncé par l'article de van Dam, Mosca, et Vazirani [5], dit que si à tout instant s :

$$\frac{\|\partial H(s)/\partial s\|}{\epsilon g^2(s)} \leq \frac{dt}{ds} \tag{15}$$

alors l'évolution est adiabatique. L'intégration de l'expression suivante permet de calculer la durée totale T nécessaire :

$$T = \int_0^T dt \geq \int_0^1 \frac{\left\| \frac{\partial H(s)}{\partial s} \right\|}{\epsilon g^2(s)} ds. \tag{16}$$

Dans le cas où il est difficile de déterminer la fonction $s(t)$, il est possible de choisir une évolution linéaire $s(t) = t/T$ avec :

$$T \geq \frac{\max_{s \in [0,1]} \|\partial H(s)/\partial s\|}{\epsilon \min_{s \in [0,1]} g^2(s)}.$$

Ce n'est pas la solution la plus efficace comme le montrera l'exemple de la section 5.

4 Implémentation par un Circuit Quantique

Maintenant il s'agit de montrer qu'il est possible d'implémenter un algorithme de calcul adiabatique à l'aide d'un circuit quantique conventionnel de taille polynomiale. Il faut d'abord montrer qu'il est possible de discrétiser l'évolution continue par une séquence finie de transformations unitaires, ensuite il est nécessaire de montrer comment réaliser ces transformations grâce à des portes quantiques élémentaires. Tout cela se résume à montrer qu'il est possible de borner l'erreur à chaque étape de ce processus d'approximation. Cette section clarifie la démonstration de l'article de van Dam, Mosca, et Vazirani [6].

Le premier lemme montre qu'il est possible d'approximer un hamiltonien $H(t)$ par un autre $H'(t)$. Si à tout instant t, l'écart entre ces deux hamiltoniens est borné, alors l'erreur entre les deux évolutions induites est bornée. Dans le cas présent, cela permet de discrétiser un hamiltonien continu par une suite d'hamiltoniens constants.

Lemme 1 *Soient $H(t)$ et $H'(t)$ deux hamiltoniens définis pour $0 \leq t \leq T$, et soient $U(t)$ et $U'(t)$ les deux transformations unitaires induites. Si à tout instant t, $\|H(t) - H'(t)\| \leq \delta$, alors $\|U(T)\,|\psi(0)\rangle - U'(T)\,|\psi(0)\rangle\| \leq \sqrt{2T\delta}$.*

Preuve. La dérivé de $\langle\psi(t)|\psi'(t)\rangle$ est :

$$\begin{aligned}
\frac{\partial}{\partial t}\langle\psi'(t)|\psi(t)\rangle &= \left(\frac{\partial}{\partial t}\langle\psi'(t)|\right)\psi(t)\rangle + \langle\psi'(t)\left(|\frac{\partial}{\partial t}\psi(t)\rangle\right) \\
&= i\,\langle\psi'(t)|H'(t)|\psi(t)\rangle - i\,\langle\psi'(t)|H(t)|\psi(t)\rangle \\
&= -i\,\langle\psi'(t)|H(t) - H'(t)|\psi(t)\rangle\,.
\end{aligned}$$

En utilisant l'inégalité de Cauchy-Schwartz, et le fait qu'à tout instant t : $\||\psi'(t)\rangle\| = \||\psi(t)\rangle\| = 1$ et $\|H(t) - H'(t)\| \leq \delta$, il vient l'inégalité :

$$\begin{aligned}
\left|\frac{\partial}{\partial t}\langle\psi'(t)|\psi(t)\rangle\right| &= |-i\,\langle\psi'(t)|H(t) - H'(t)|\psi(t)\rangle\,| \\
&\leq \||\psi'(t)\rangle\|\cdot\|H(t) - H'(t)\,|\psi(t)\rangle\| \\
&\leq \|H(t) - H'(t)\,|\psi(t)\rangle\| \\
&\leq \delta.
\end{aligned}$$

Dont l'intégration donne :

$$|\,\langle\psi'(t)|\psi(t)\rangle\,| \leq \left|\int_0^T \delta\,dt\right| = T\delta,$$

en utilisant la condition initiale $\langle\psi(0)|\psi(0)\rangle = 1$, il est possible de conclure que :

$$|\,\langle\psi'(T)|\psi(T)\rangle\,| \geq 1 - T\delta.$$

En utilisant l'inégalité précédente, il est possible de borner l'écart entre les deux transformations induites :

$$\begin{aligned}
\|U(T)\,|\psi(0)\rangle - U'(T)\,|\psi(0)\rangle\| &= \||\psi(T)\rangle - |\psi'(T)\rangle\| \\
&= \sqrt{\langle\psi(T) - \psi'(T)|\psi(T) - \psi'(T)\rangle} \\
&= \sqrt{2 - 2\Re\,\langle\psi(T)|\psi'(T)\rangle} \\
&\leq \sqrt{2T\delta}.
\end{aligned}$$

□

Dans le cas où A et B ne commutent pas, le second lemme montre qu'il est possible d'approximer $e^{t(A+B)}$ par $e^{tA}e^{tB}$ sans introduire trop d'erreur. Dans notre cas, cela permet de calculer une évolution unitaire de la forme $e^{t(A+B)}$ à l'aide d'un circuit $e^{tA}e^{tB}$ plus facile à réaliser.

Lemme 2 *Soient A et B deux matrices quelconques, et soit $t \to 0$, alors $e^{t(A+B)} - e^{tA}e^{tB} \in O(t^2AB)$.*

Preuve. Il est possible d'utiliser l'approximation asymptotique suivante :

$$e^{tM} = I + tM + O(t^2M^2)$$

car $t \to 0$. La suite est un simple calcul :

$$\begin{aligned} e^{t(A+B)} - e^{tA}e^{tB} &= I + t(A+B) + O(t^2(A+B)^2) - (I + tA + O(t^2A^2))(I + tB + O(t^2B^2)) \\ &= O(t^2AB) - t^2AB - O(t^3AB^2) - O(t^3A^2B) - O(t^4A^2B^2) \\ &= O(t^2AB). \end{aligned}$$

□

Le troisième lemme montre qu'il est possible d'approximer une séquence de transformations unitaires par une autre. Si pour chaque transformation unitaire, la différence entre la transformation exacte et l'approximation est bornée, l'erreur totale est bornée. Ici, cela montre qu'il est possible d'utiliser des approximations de circuits, par exemple celui proposé par le lemme 2.

Lemme 3 *Soient U_j et U'_j deux transformations unitaires définis pour $1 \leq j \leq r$, et soit $|\psi_r\rangle = U_{r-1} \cdots U_2U_1 |\psi_0\rangle$ et $|\psi'_r\rangle = U'_{r-1} \cdots U'_2U'_1 |\psi_0\rangle$ les deux vecteurs finaux. Si pour tout j, $\left\|U_j - U'_j\right\| \leq \delta$, alors $\||\psi_r\rangle - |\psi'_r\rangle\| \leq r\delta$.*

Preuve. Soit

$$|\psi_j\rangle = U_j |\psi_{j-1}\rangle = |\psi'_j\rangle + |E_j\rangle = U'_j |\psi_{j-1}\rangle + |E_j\rangle,$$

de ce fait

$$(U_j - U'_j) |\psi_{j-1}\rangle = |E_j\rangle$$

où $|E_j\rangle$ est un vecteur non normalisé. Le résultat d'une suite de transformations unitaires U_j est :

$$\begin{aligned} |\psi_r\rangle &= U_{r-1} \cdots U_2U_1 |\psi_0\rangle \\ &= U'_{r-1} \cdots U'_2U'_1 |\psi_0\rangle + |E_r\rangle + U'_{r-1} |E_{r-1}\rangle + \cdots + U'_{r-1} \cdots U'_2 |E_1\rangle. \end{aligned}$$

En utilisant l'inégalité triangulaire : $\|x + y\| \leq \|x\| + \|y\|$, et l'hypothèse $\left\|U_j - U'_j\right\| \leq \delta$, il est possible de conclure que :

$$\begin{aligned} \|\psi_r - \psi'_r\| &= \left\||E_r\rangle + U'_{r-1} |E_{r-1}\rangle + \cdots + U'_{r-1} \cdots U'_2 |E_1\rangle\right\| \\ &\leq \||E_r\rangle\| + \||E_{r-1}\rangle\| + \cdots + \||E_1\rangle\| \\ &\leq r\delta. \end{aligned}$$

□

Le dernier lemme montre comment construire un circuit quantique réalisant un changement de phase contrôlé par une fonction $f(x)$. C'est utile car l'évolution unitaire d'un hamiltonien indépendent du temps correspond à un changement de phase.

Définition 4 (Porte U_f) *Soient respectivement deux registres $|x\rangle$ et $|y\rangle$ de n et k qubits, et soit une fonction $f(x) : \{0,1\}^n \to \{0,1\}^k \in O(n^d)$. La porte quantique U_f réalise l'opération : $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. Cette porte est supposée être de complexité polynomiale en temps et en espace.*

Définition 5 (Porte de changement de phase $C_{\alpha,j}$) *Soient respectivement deux registres $|x\rangle$ et $|y\rangle$ de n et k qubits. La porte quantique $C_{\alpha,j}$ réalise l'opération de changement de phase contrôlé : $C_{\alpha,j} |x\rangle |y\rangle = e^{iy_j\alpha 2^j} |x\rangle |y\rangle$, où y_j correspond au bit j du registre $|y\rangle$. Cette porte est supposée être de complexité polynomiale en temps et en espace.*

Lemme 4 *Soient deux registres $|x\rangle$ et $|y\rangle$ de respectivement n et k qubits, et soit une fonction $f(x)$: $\{0,1\}^n \to \{0,1\}^k$. La séquence de portes quantiques $U_f(\prod_{j=0}^{k-1} C_{\alpha,j})U_f$ réalise l'opération : $F_{\alpha,f(x)} |x\rangle = e^{i\alpha f(x)} |x\rangle$. Cette suite de portes est de complexité polynomiale en temps et en espace.*

Preuve. Dans le cas où $k = 1$, c'est-à-dire où $f(x)$ est une fonction binaire, le calcul est assez simple. Soit :

$$|x\rangle\,|y\rangle = \left(\sum_{i=0}^{2^n-1} c_i\,|i\rangle\right) \otimes |0\rangle\,,$$

en appliquant l'opérateur linéaire U_f l'expression devient:

$$U_f\,|x\rangle\,|y\rangle = \sum_{i=0}^{2^n-1} c_i\,|i\rangle\,|f(i)\rangle\,,$$

et en appliquant $C_{\alpha,0}$:

$$C_{\alpha,0}U_f\,|x\rangle\,|y\rangle = \sum_{i=0}^{2^n-1} e^{i\alpha f(i)}c_i\,|i\rangle\,|f(i)\rangle\,.$$

Les opérations précédentes ont seulement modifié la phase de $|x\rangle$, aussi il suffit d'appliquer U_f pour remettre le registre $|y\rangle$ dans son état initial. Dans le cas général où k est quelconque, il suffit d'appliquer k fois l'opérateur $C_{\alpha,j}$, une fois pour chaque qubit j de $|y\rangle$, l'idée est de décomposer $f(x)$ en base 2. La complexité polynomiale en temps et en espace se déduit de manière immédiate. □

Avec ces lemmes et en utilisant les mêmes hypothèses que la section 3, excepté que $h(z)$ et $f(z)$ sont des fonctions de $\{0,1\}^n$ dans $\{0,1\}^k$ au lieu de $\mathbf{R}$, il est possible de montrer que le calcul adiabatique est implémentable par un circuit quantique conventionnel.

Theorème 4 *Soient $f(z) \in O(n^d)$ et $h(z) \in O(n^{d'})$. Soient respectivement*

$$H_0 = \sum_{z\in\{0,1\}^n} h(z)\,|\bar{z}\rangle\langle\bar{z}| \qquad et \qquad H_1 = \sum_{z\in\{0,1\}^n} f(z)\,|z\rangle\langle z|$$

les hamiltoniens initial de base $|\bar{z}\rangle$ et final de base $|z\rangle$. Soit l'hamiltonien $H(t) = (1-s(t))H_0 + s(t)H_1$ faisant évoluer le système de $t = 0$ à $t = T$. $U(T)$ est la transformation unitaire induite. Soient respectivement B_0 et B_1 les transformations unitaires permettant de passer des bases $|z\rangle$ à $|\bar{z}\rangle$ et $|\bar{z}\rangle$ à $|z\rangle$. B_0 et B_1 sont supposées implémentables par des circuits de complexité polynomiale en temps et en espace.

Avec ces hypothèses, il est possible d'approximer $U(T)$ par une séquence de $r \in O(T^2n^{d+d'})$ transformations unitaires de la forme $B_0F_{\alpha,h(z)}B_1F_{\beta,f(z)}$. Cette approximation peut s'effectuer avec une complexité polynomiale en temps et en espace.

Preuve. Le lemme 1 nous permet de discrétiser un hamiltonien $H(t)$ continu par une suite de r hamiltoniens H'_j constants de durée T/r, soit $H'(t) = H'_{\lceil \frac{rt}{T}\rceil}$ cette suite. Pour $1 \le j \le r$, les hamiltoniens H'_j sont de la forme :

$$H'_j = H(jT/r) = (1 - s(jT/r))H_0 + s(jT/r)H_1,$$

ce qui induit une transformation unitaire :

$$U'_j = \exp -\frac{i}{\hbar}\left(\frac{T}{r}\,[(1 - s(jT/r))H_0 + s(jT/r)H_1]\right).$$

$H'(t)$ induit l'évolution unitaire :

$$U'(T) = U'_j \cdots U'_2U'_1.$$

Comme $\|H(t) - H(t')\| \le \frac{1}{r}\,\|H_1 - H_0\| \in O((n^d - n^{d'})/r)$, le lemme 1 permet de conclure que :

$$\|U(T) - U'(T)\| \in O(\sqrt{T(n^d - n^{d'})/r}).$$

Réaliser U'_j avec un circuit quantique est difficile, en revanche :

$$U''_j = \exp -\frac{i}{\hbar}[(T/r)(1 - s(jT/r))H_0] \times \exp -\frac{i}{\hbar}[(T/r)s(jT/r)H_1]$$

correspond à une séquence de deux changements de phase. De plus, le lemme 2 montre que lorsque $(T/r) \to 0$, l'erreur est bornée : $\|U'_j - U''_j\| \in O(\frac{T^2}{r^2}\|H_0 H_1\|) = O(\frac{T^2}{r^2}n^{d+d'})$. Soit $U''(T)$ l'évolution unitaire obtenue en utilisant cette approximation, le lemme 3 donne l'erreur totale : $\|U'(T) - U''(T)\| \in O(\frac{T^2}{r}n^{d+d'})$, ce qui permet de conclure :

$$
\begin{aligned}
\|U(T) - U''(T)\| &= \|U(T) - U'(T)\| + \|U'(T) - U''(T)\| \\
&\in O(\sqrt{T(n^d - n^{d'})}/r) + O(\frac{T^2}{r}n^{d+d'}) \\
&\in O(\frac{T^2}{r}n^{d+d'}).
\end{aligned}
$$

Pour réaliser U''_j, il suffit d'aller dans la base de H_0 d'effectuer le changement de phase, puis de retourner dans celle de H_1 et d'effectuer le second changement de phase :

$$U''_j = B_0 F_{(T/r)(1-s(jT/r)),h(z)} B_1 F_{(T/r)s(jT/r),f(z)}.$$

Avec les hypothèses de l'énoncé, chaque transformation unitaire U''_j peut être réalisée en temps et en espace polynomial, comme la taille du circuit ne dépend que de r, la complexité en temps et en espace du circuit complet est polynomiale en T et n. □

Il est à noter que la simulation induit un surcoût quadratique en T.

5 Application: Recherche

Le problème est le suivant : il s'agit de trouver un élément marqué m parmis N éléments rangés sans ordre particulier. Pour cela, il suffit d'utiliser n qubits, ce qui donne un espace de Hilbert de dimension $N = 2^n$ dont les états sont les kets $|i\rangle$ avec $i \in [0, N-1]$. L'élément marqué correspond à l'état $|m\rangle$. Soient :

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

et les deux hamiltoniens :

$$
\begin{aligned}
H_0 &= I - |\psi_0\rangle\langle\psi_0| \\
H_1 &= I - |m\rangle\langle m|
\end{aligned}
$$

dont les états fondamentaux sont respectivement $|\psi_0\rangle$ et $|m\rangle$ Il est à noter que pour toute base $|x\rangle$:

$$\sum_{x \in \{0,1\}^N} |x\rangle\langle x| = I.$$

L'hamiltonien H_0 est défini dans la base d'Hadamard $|\bar{z}\rangle$:

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{et} \qquad |\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

et H_1 dans la base de calcul $|z\rangle$ usuelle. L'hamiltonien initial est H_0 car son état fondamental est connu. En revanche, l'état $|m\rangle$ n'est a priori pas connu, H_1 est donc l'hamiltonien final. Si l'évolution est adiabatique, une mesure donnera avec grande probabilité le vecteur $|m\rangle$ au temps T.

Tout d'abord, il faut calculer les valeurs propres de l'hamiltonien :

$$H(t) = f(t)H_0 + g(t)H_1,$$

où $f(t) = 1 - s(t)$ et $g(t) = s(t)$, pour alléger l'écriture la variable t sera omise. Pour cela, il suffit de déterminer les solutions de l'équation caractéristique : $\det(H - I\lambda) = 0$. Soit $a = f + g - \lambda$, $b = f - \lambda$, et $c = -(1/N)f$. Soit $i, j \in [0, N-1]$, $H - I\lambda$ est une matrice de la forme suivante (les colonnes et lignes sont numérotées à partir de 0) :

1. si $i \neq j$, alors $a_{ij} = c$;
2. si $i = j = m$, alors $a_{ii} = b + c$, sinon $a_{ii} = a + c$.

Par exemple, dans le cas où $m = 2$ et $N = 4$:

$$H - I\lambda = \begin{pmatrix} a+c & c & c & c \\ c & a+c & c & c \\ c & c & b+c & c \\ c & c & c & a+c \end{pmatrix}.$$

Pour calculer le déterminant, il suffit de permuter lignes et colonnes pour que le coefficient de la forme $b + c$ soit à la position du coefficient a_{00}, puis de soustraire la colonne 0 aux $N - 1$ autres colonnes, en reprenant notre exemple, la matrice devient :

$$\begin{pmatrix} b+c & -b & -b & -b \\ c & a & 0 & 0 \\ c & 0 & a & 0 \\ c & 0 & 0 & a \end{pmatrix}.$$

Il suffit ensuite de développer par rapport à la première ligne. Au final, le calcul du déterminant se résume à résoudre l'équation :

$$\det(H - I\lambda) = [(b+c)a + (N-1)bc]a^{N-2} = 0.$$

Il y a trois valeurs propres :

$$\begin{aligned} E_0 &= \frac{1}{2}\left(1 - \sqrt{1 - 4\left(\frac{N-1}{N}\right)s(1-s)}\right), \\ E_1 &= \frac{1}{2}\left(1 + \sqrt{1 - 4\left(\frac{N-1}{N}\right)s(1-s)}\right), \\ E_2 &= 1, \end{aligned}$$

E_2 a une multiplicité de $N - 2$. L'écart d'énergie minimum est donc :

$$g(s) = \sqrt{1 - 4\left(\frac{N-1}{N}\right)s(1-s)}.$$

Comme les valeurs propres de H_0 et H_1 sont aux plus égals à 1, et que :

$$\frac{\partial H(s)}{\partial s} = H_1 - H_0,$$

il est possible d'effectuer la majoration suivante :

$$\left\| \frac{\partial H(s)}{\partial s} \right\| \leq 1,$$

ce qui permet d'aboutir à l'inégalité :

$$\frac{dt}{ds} \geq \frac{1}{\epsilon g^2(s)} \geq \frac{\|\partial H(s)/\partial s\|}{\epsilon g^2(s)}.$$

Grâce à cette dernière inégalité, il est possible de déterminer la fonction $s(t)$ permettant de minimiser la durée T de l'évolution. Le temps t est donnée par l'intégrale :

$$t = \int_0^t dt = \frac{1}{\epsilon}\int_0^s \frac{ds}{g^2(s)} = \frac{N}{\epsilon}\int_0^s \frac{ds}{N + 4(N-1)s(s-1)}.$$

Il suffit d'effectuer un changement de variable, en prenant : $u = \sqrt{N-1}(2s-1)$, l'intégrale devient :

$$t = \frac{N}{2\epsilon\sqrt{N-1}} \int_{u(0)}^{u(s)} \frac{du}{1+u^2} = \frac{N}{2\epsilon\sqrt{N-1}} \left[\arctan(\sqrt{N-1}(2s-1)) + \arctan(\sqrt{N-1})\right]. \qquad (17)$$

Pour obtenir $s(t)$, il suffit d'inverser la fonction précédente :

$$s(t) = \frac{1}{2\sqrt{N-1}} \left(\tan\left[\frac{2\epsilon\sqrt{N-1}}{N}t - \arctan(\sqrt{N-1}\right] + \sqrt{N-1}\right).$$

Au final, (17) donne :

$$T = \frac{N}{\epsilon} \frac{\arctan(\sqrt{N-1})}{\sqrt{N-1}},$$

comme $N \gg 1$, alors :

$$T \approx \frac{\pi}{2\epsilon}\sqrt{N},$$

c'est la même complexité que l'algorithme de Grover [7]. Malheureusement, la simulation par un circuit quantique induit un surcoût quadratique en T, ce qui rend la complexité linéaire en $O(N)$.

Cette section a vérifié les calculs de l'article de Roland et Cerf [8].

6 Conclusion

Le calcul quantique par évolution adiabatique est un nouveau modèle de calcul équivalent aux circuits quantiques conventionnels. En effet, il est possible de simuler une évolution adiabatique avec une complexité polynomiale en temps et en espace. En appliquant le calcul adiabatique au problème de recherche, il est possible de retrouver la complexité $O(\sqrt{N})$ de l'algorithme de Grover, malheureusement la simulation par un circuit quantique induit un surcoût quadratique en T qui le transforme en algorithme linéaire en $O(N)$. Il serait donc très intéressant de chercher des méthodes de simulation plus efficace.

Remerciement L'auteur souhaite remercier Frédéric Magniez d'avoir encadré ce stage de DEA. La référence [3] a été suggérée par Pranab Sen. L'auteur tient aussi à remercier tous les membres de l'équipe Algorithmique et Complexité du Laboratoire de Recherche en Informatique d'Orsay pour leur accueil, leur aide, et surtout leur gentillesse.

7 Références

[1] Claude Cohen-Tannoudji, Bernard Diu, Franck Laloë, *Mécanique Quantique*, Tome I, Hermann, Paris, 1973.

[2] Albert Messiah, *Mécanique Quantique*, Tome II, Dunod, Paris, 1964.

[3] Jenn-Tai Hwang, Philip Pechukas, *The Adiabatic Theorem in the complex plane and the semiclassical calculation of nonadiabatic transition amplitudes*, J. of Chemical Physics, Volume 67, p4640, 1977.

[4] Leonard I. Schiff, *Quantum Mechanics*, McGraw-Hill, New York, 1968.

[5] Wim van Dam, Michele Mosca, Umesh Vazirani, *How Powerful is Adiabatic Quantum Computation?*, Proc. 32th FOCS, p279, IEEE Press, 2001.

[6] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Michael Sipser, *Quantum Computation by Adiabatic Evolution*, MIT CTP # 2936, quant-ph/0001106, 2000.

[7] Michael A. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[8] Jérémie Roland, Nicolas J. Cerf, *Quantum Search by Local Adiabatic Evolution*, quant-ph/0107015, 2001.