INF581: Information Quantique **Hiver 2010**

Cours 6 — 15 février

Enseignant : P. Grangier – F. Magniez *Rédacteur : B. Crespin – N. Galtier*

6.1 Algorithme de Grover

6.1.1 Formulation du problème

Soit f une fonction de $\{0,1\}^n \to \{0,1\}$, telle qu'il existe un unique $x_0 \in \{0,1\}^n$ pour lequel $f(x_0) = 1$. On cherche ce x_0. Le meilleur algorithme classique consiste à calculer $f(x)$ pour tout x. Sa complexité est donc linéaire dans le pire des cas.

6.1.2 Notations

On se place dans un espace d'état à $N = 2^n$ dimensions dont on note $\{|x\rangle | x \in \{0,1\}^n\}$ une base. Cela peut par exemple être obtenu en considérant n qubits.

On associe à f l'opérateur S_f suivant :

$$S_f : \sum_x a_x |x\rangle \longmapsto \sum_x (-1)^{f(x)} a_x |x\rangle$$

On a le lemme suivant :

Lemme 6.1. *Pour tout $x \in \{0,1\}^n$,*

$$S_f|x_0\rangle = -|x_0\rangle$$

$$S_f|x\rangle = |x\rangle \text{ si } |x\rangle \neq |x_0\rangle$$

On rappelle la propriété suivante de la porte de Hadamard :

Lemme 6.2.

$$H^{\otimes n}|x\rangle = \sum_y (-1)^{x.y} |y\rangle$$

où $x.y$ désigne le produit scalaire modulo 2.

6.1.3 Algorithme

On définit l'opérateur de Grover par :

$$G = S_f H^{\otimes n} (-S_{\delta_0}) H^{\otimes n}$$

On part de l'état initial uniforme $|u\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = H^{\otimes n}|0\rangle$ et on itère G.

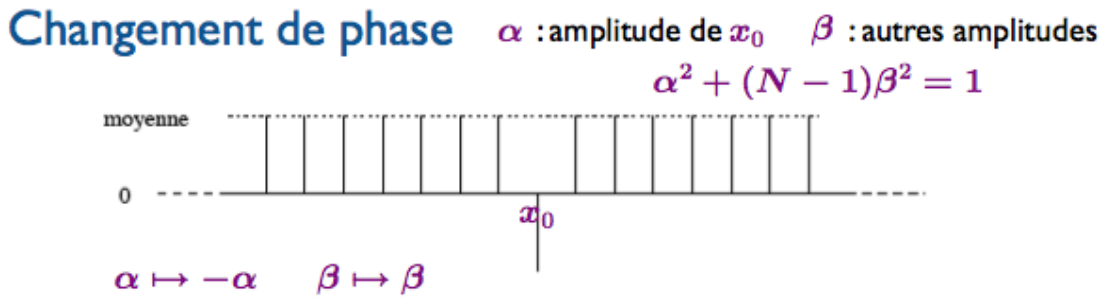

Figure 6.1. S_f change la phase associée au vecteur $|x_0\rangle$ et laisse les autres amplitudes inchangées.

L'opérateur de Grover agit en deux temps :
- comme vu dans le lemme 6.1, S_f change la phase associée au vecteur recherché $|x_0\rangle$ et laisse inchangées les autres amplitudes.

- $H^{\otimes n}(-S_{\delta_0})H^{\otimes n}$ inverse l'amplitude associée à chaque vecteur de la base, par rapport à la moyenne des amplitudes.

On voit qu'en itérant cet opérateur, l'amplitude de la composante $|x_0\rangle$ augmente par rapport à la moyenne des amplitudes des autres composantes.

6.1.4 Preuve

La preuve de l'algorithme de Grover repose sur la remarque précédente.
Soient α_k et β_k tels que $G^k|u\rangle = \alpha_k|x_0\rangle + \beta_k \sum_{x\neq x_0} |x\rangle$. On a $\alpha_0 = \beta_0 = \frac{1}{\sqrt{N}}$.

Changement de phase

D'après le lemme 6.1,

$$S_f(\alpha_k|x_0\rangle + \beta_k \sum_{x\neq x_0} |x\rangle) = -\alpha_k|x_0\rangle + \beta_k \sum_{x\neq x_0} |x\rangle$$

S_f inverse donc la phase associée au vecteur $|x_0\rangle$, comme illustré sur la figure 6.1.

Inversion des amplitudes

On applique ensuite $H^{\otimes n}(-S_{\delta_0})H^{\otimes n}$.

$$H^{\otimes n}(-S_{\delta_0})H^{\otimes n}[-\alpha_k|x_0\rangle + \beta_k \sum_{x\neq x_0} |x\rangle] = \alpha_{k+1}|x_0\rangle + \beta_{k+1} \sum_{x\neq x_0} |x\rangle$$

avec $\alpha_{k+1} = \alpha_k + 2\beta_k - \frac{2}{N}(\beta_k + \alpha_k)$ et $\beta_{k+1} = \beta_k - \frac{2}{N}(\beta_k + \alpha_k)$. La figure 6.2 illustre l'inversion des amplitudes par rapport à la moyenne des amplitudes $\frac{(N-1)\beta_k + \alpha_k}{N}$.

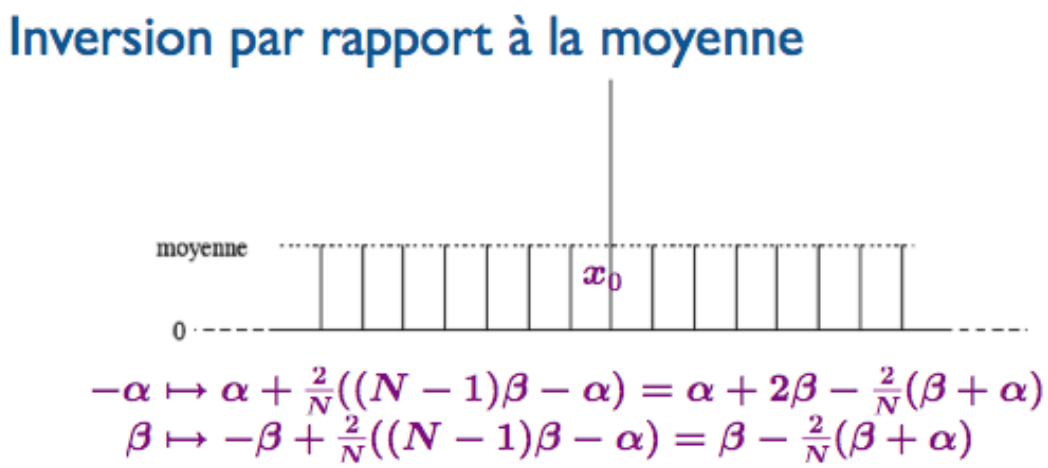

Figure 6.2. $H^{\otimes n}(-S_{\delta_0})H^{\otimes n}$ inverse toutes les amplitudes par rapport à la moyenne.

Convergence

Les suites $(\alpha_k)_k$ et $(\beta_k)_k$ vérifient :

$$\alpha_{k+1} = \alpha_k + 2\beta_k - \frac{2}{N}(\beta_k + \alpha_k)$$

$$\beta_{k+1} = \beta_k - \frac{2}{N}(\beta_k + \alpha_k)$$

$$\alpha_0 = \beta_0 = \frac{1}{\sqrt{N}}$$

Les formes explicites de $(\alpha_k)_k$ et $(\beta_k)_k$ sont alors :

$$\alpha_k = \sin(2k+1)\theta$$

$$\beta_k = \cos(2k+1)\theta$$

avec $\sin\theta = \frac{1}{\sqrt{N}}$.

On veut α proche de 1, soit $(2k+1)\theta \approx \frac{\pi}{2} \Leftrightarrow k \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$. Le nombre d'itérations nécessaires est donc de l'ordre de $\frac{\pi}{4}\sqrt{N}$ et la complexité de l'algorithme de Grover est en $O(\sqrt{N})$.

6.1.5 Cas de plusieurs solutions

On suppose maintenant qu'il existe exactement t solutions, c'est-à-dire t éléments distincts $(x_0, ..., x_t)$ de $\{0,1\}^n$ tels que $f(x_i) = 1$. Nous cherchons à trouver une seule de ces solutions.

Le nombre t de solution est connu.

Il suffit alors de considérer la superposition des t états correspondants aux solutions comme un seul état avec une amplitude $\sqrt{\frac{K}{N}}$. On se ramène alors au problème consistant à trouver une solution parmi $\frac{N}{K}$ possibilités. L'algorithme de Grover résout le problème avec une complexité en $O(\sqrt{\frac{N}{K}})$.

Le nombre t de solution est inconnu.

Nous admettons que l'algorithme suivant résout le problème avec une complexité *en moyenne* en $O(\sqrt{\frac{N}{K}})$.

Initialisation :
– m=1.
Boucle :
– choisir aléatoirement j dans $\{1, ..., m-1\}$;
– appliquer j fois l'opérateur de Grover à l'état uniforme $|u\rangle$.
Condition d'arrêt :
– si le résultat i a une image 1 par f, on rend i ;
– sinon, on continue avec $m = \min(\frac{8}{7}m, \sqrt{N})$.

6.1.6 Optimalité

Soit U un algorithme quantique de recherche qui résout le problème de Grover avec précision ϵ. U est une alternance d'appel à S_f et d'opérateurs unitaires :

$$U = U_T S_f U_{T-1} S_f ... U_1 S_f U_0$$

On définit les fonctions f_i pour $i \in \{0, ..., N\}$ suivantes.
Pour tout $x \in \{1, ..., N\}$,

$$f_0|x\rangle = 0$$
$$f_i|x\rangle = \delta_{x,i}$$

La réponse de l'algorithme doit donc être i si on l'applique avec la fonction f_i où $i \neq 0$ et l'algorithme ne renvoie pas de solution si on l'applique à f_0. On note $|\psi_i^t\rangle$ l'état après avoir appelé t fois S_f dans l'algorithme.

On mesure le progrès de l'algorithme par la somme des produits scalaires des états du circuit dans les cas f_i et l'état du circuit dans le cas f_0 :

$$W_t = \sum_{i=1}^{N} |\langle \psi_0^t || \psi_i^t \rangle|$$

Conditions initiales et finales

On a initialement $W_0 = N$. Les états finaux étant quasi-orthogonaux, on a finalement : $|\langle \psi_0^T || \psi_i^T \rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}$, soit $W_T \leq 2N\sqrt{\epsilon(1-\epsilon)}$.

Intéressons-nous maintenant à l'évolution de W entre les instants t et $t+1$.

Appels des U_k

Les applications unitaires U_k ne changent pas le produit scalaire $\langle\psi_0^t||\psi_i^t\rangle$, car :

$$\langle\psi_0^t||\psi_i^t\rangle = \langle\psi_0^t U_t||U_t\psi_i^t\rangle$$

Appels de S_{f_i}

$$|\langle\psi_0^t||\psi_i^t\rangle - \langle\psi_0^{t+1}||\psi_i^{t+1}\rangle| = |\langle\psi_0^t||\psi_i^t\rangle - \langle\psi_0^t|S_{f_i}|\psi_i^t\rangle| \leq 2|\langle\psi_0^t|P_i|\psi_i^t\rangle| \leq 2||P_i|\psi_0^t\rangle||$$

en notant P_i le projecteur sur le sous espace posant la question i.

On a donc :

$$|W_t - W_{t+1}| \leq \sum_{i=1}^{N} 2||P_i|\psi_0^t\rangle|| \leq 2\sqrt{N}\sqrt{\sum_{i=1}^{N}||P_i|\psi_0^t\rangle||^2} = 2\sqrt{N}$$

soit $W_T \geq W_0 - 2T\sqrt{N}$. En utilisant les conditions initiales et finales, on en déduit que $2N\sqrt{\epsilon(1-\epsilon)} \geq N - 2T\sqrt{N}$, soit :

$$T \geq \frac{1 - 2\sqrt{\epsilon(1-\epsilon)}}{2}\sqrt{N}$$

L'algorithme de Grover est donc optimal en ce sens que tout autre algorithme de recherche quantique a une complexité qui est au moins en $O(\sqrt{N})$.