

Chapitre 7

Algorithme de Grover

Dans ce chapitre nous étudions un algorithme entièrement différent des précédents, qui s'applique à des objets sans structure ou sans symétrie (il n'y a pas de sous groupe caché, pas de période, etc...). Il s'agit d'un algorithme avec oracle qui effectue la recherche d'un *élément marqué* dans un *ensemble ou base de donnée sans structure*. Donnons un exemple concret.

Prenons un annuaire (la base de donnée) et supposons que les numéros de téléphone jouent le rôle des entrées, les personnes correspondantes jouent le rôle des sorties. Etant donné une entrée (le numéro de téléphone) il est difficile de retrouver la sortie (le nom de la personne correspondante). La seule façon de procéder est de faire une recherche exhaustive ou bien de procéder à une recherche aléatoire. Ces deux méthodes requièrent de soumettre $O(N)$ questions à l'annuaire où N est le nombre d'entrées. Donc si $N = 2^n$, c'est à dire que l'on peut décrire tout l'annuaire avec n bits, le temps de recherche est exponentiel $O(2^n)$. La raison fondamentale étant que la liste des numéros de téléphone n'est pas ordonnée et ne possède aucune structure. Bien sûr, le problème consistant à rechercher le téléphone d'une personne connaissant son nom est facile car la liste des noms est ordonnée par ordre alphabétique et possède donc une structure.

Nous verrons que l'algorithme de Grover permet de résoudre le problème en un temps $O(\sqrt{N}) = O(2^{\frac{n}{2}})$. Le temps est toujours exponentiel mais pour N assez grand, nous obtenons grâce au calcul quantique, une accélération quadratique. Il est possible de montrer que si le problème n'a pas de structure spéciale sous-jacente, il n'est pas possible de faire mieux que $O(\sqrt{N})$ dans le cadre du modèle de Deutsch des circuits quantiques (le facteur limitant provient de l'unitarité de l'évolution).

Remarque : reconsidérons le problème de la factorisation d'un entier $N = p \cdot q$ avec deux facteurs premiers. Il n'est pas possible d'avoir p et q supérieurs à

\sqrt{N} , donc l'un des deux est $\leq \sqrt{N}$. En cherchant à travers la liste $\{1, 2, \dots, \sqrt{N}\}$ nous trouverons sûrement un des deux facteurs premiers. Avec une recherche exhaustive il faut un temps \sqrt{N} , mais avec l'algorithme de Grover (ici l'oracle serait une boîte noire testant la division de N par $x \in \{1, 2, \dots, \sqrt{N}\}$; bien sur l'algorithme d'euclide ferait l'affaire) il faut un temps $O(N^{1/4})$ ce qui est déjà amusant. Nous savons qu'il est possible de faire mieux (même classiquement) et d'obtenir une accélération exponentielle grâce à l'algorithme de Shor, mais cela n'est possible qu'en exploitant la symétrie (la périodicité) d'une fonction arithmétique liée au problème de la factorisation.

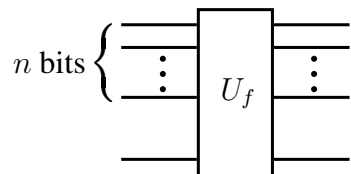
7.1 Formulation Mathématique du Problème

Soit $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 = \{0, 1\}$ et soit l'équation

$$f(x_1, \dots, x_n) = 1.$$

Nous voulons déterminer au moins une solution x_1^*, \dots, x_n^* , parmi les 2^n entrées possibles. Nous ne voulons pas déterminer toutes les solutions possibles, mais simplement l'une d'entre elles. L'application typique qui nous intéresse est celle où il y a une solution unique et où n est grand. Nous exigeons de connaître à priori le nombre total de solutions. Mais cette restriction peut ensuite être supprimée grâce à une extension facile de l'algorithme de base. On notera $(x_1, \dots, x_n) = \underline{x}$.

Nous supposons avoir à disposition un oracle quantique :



$$U_f |\underline{x}\rangle \otimes |b\rangle = |x\rangle \otimes |b \oplus f(\underline{x})\rangle$$

$\underline{x} \in \mathbb{F}_2^n$ et $b = 0$ ou 1 .

Le lecteur constatera la généralité du problème formulé ci-dessus.

7.2 Dérivation de l'algorithme

Dans les chapitres précédents nous avons toujours commencé par donner le circuit de l'algorithme. Cette fois nous procédons de façon plus inductive, et verrons que l'algorithme de Grover peut être construit de façon assez

naturelle. L'état initial entrant dans le circuit est :

$$|\underbrace{0 \dots 0}_{n \text{ fois}}\rangle \otimes |1\rangle$$

où les n premiers qubits stockent les entrées et le dernier bit est un bit auxiliaire. Pour exploiter le parallélisme quantique nous formons une superposition cohérente sur toutes les entrées possibles (grâce aux portes de Hadamard agissant sur tous les qubits du premier registre) :

$$(H \otimes \dots \otimes H) \otimes \mathbf{1}|0 \dots 0\rangle \otimes |1\rangle = \frac{1}{2^{n/2}} \sum_{\underline{x} \in \mathbb{F}_2^n} |\underline{x}\rangle \otimes |1\rangle.$$

L'opération de Hadamard sur le second registre se révèle être utile ci-dessous (pour obtenir le phénomène *kick-back phase*). L'état devient alors :

$$\frac{1}{2^{n/2}} \sum_{\underline{x} \in \mathbb{F}_2^n} |\underline{x}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Appliquons maintenant U_f , ce qui conduit à

$$\frac{1}{2^{n/2}} \sum_{\underline{x} \in \mathbb{F}_2^n} |\underline{x}\rangle \otimes \frac{1}{\sqrt{2}}(|f(\underline{x})\rangle - |1 \oplus f(\underline{x})\rangle).$$

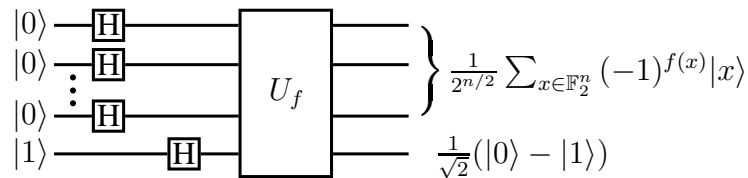
On note que

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

ce qui permet de repr'esenter ce dernier état comme

$$\frac{1}{2^{n/2}} \sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{f(\underline{x})} |\underline{x}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Les opérations effectuées ci-dessus sont résumées dans la figure :



Nous voyons que la solution de l'équation $f(\underline{x}) = 1$ a été *marquée* d'une phase égale à -1 (ou π) dans l'état résultant.

Discutons maintenant une interprétation géométrique des opérations faites jusqu'ici. Soit M le nombre de solutions de l'équation $f(\underline{x}) = 1$, et soit deux états quantiques

$$|S\rangle = \frac{1}{\sqrt{M}} \sum_{\underline{x} \text{ sol}} |\underline{x}\rangle,$$

$$|P\rangle = \frac{1}{\sqrt{N-M}} \sum_{\underline{x} \text{ pas sol}} |\underline{x}\rangle.$$

On peut alors voir que :

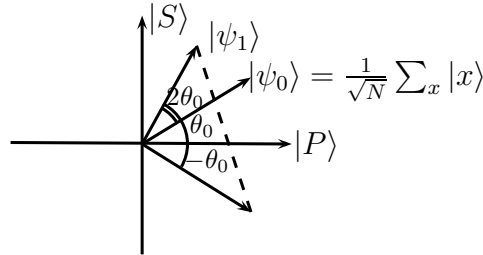
$$\frac{1}{\sqrt{N}} \sum_{\underline{x}} |\underline{x}\rangle = \sqrt{\frac{M}{N}} |S\rangle + \sqrt{\frac{N-M}{N}} |P\rangle,$$

$$\frac{1}{\sqrt{N}} \sum_{\underline{x}} (-1)^{f(\underline{x})} |\underline{x}\rangle = -\sqrt{\frac{M}{N}} |S\rangle + \sqrt{\frac{N-M}{N}} |P\rangle.$$

Puisque $\sqrt{\frac{M}{N}} + \sqrt{\frac{N-M}{N}} = 1$ nous pouvons définir un angle θ_0 tel que

$$\sin \theta_0 = \sqrt{\frac{M}{N}} \quad \text{et} \quad \cos \theta_0 = \sqrt{\frac{N-M}{N}}.$$

L'entrée du premier registre est un vecteur dans le plan $\{|P\rangle, |S\rangle\}$ formant un angle θ_0 avec l'axe $|P\rangle$. La sortie est le vecteur obtenu par réflexion par rapport à $|P\rangle$ et formant l'angle $-\theta_0$ avec ce dernier.



L'état réfléchi contient les solutions marquées par une phase -1.

La prochaine étape consiste en une réflexion par rapport à $|\psi\rangle_0$, ce qui nous amène sur $|\psi\rangle_1$. On notera deux points importants :

- En obtenant $|\psi\rangle_1$ on s'est rapproché de $|S\rangle$ (au moins si θ_0 était faible au départ, donc $M \ll N$).
- La réflexion est faite par rapport à $|\psi\rangle_0$ et n'utilise aucune information sur les solutions (inconnues).

Nous avons

$$|\psi_1\rangle = \cos 3\theta_0|P\rangle + \sin 3\theta_0|S\rangle.$$

Le troisième point à remarquer est :

- $|\psi_1\rangle$ est une rotation d'angle $2\theta_0$ de $|\psi_0\rangle$ dans le plan $\{|P\rangle, |S\rangle\}$.

En itérant ce procédé - réflexion autour de $|P\rangle$, puis réflexion autour de $|\psi_0\rangle$ - on obtient la suite d'états obtenus par rotations successives d'angle $2\theta_0$:

$$|\psi_K\rangle = \cos(2K + 1)\theta_0|P\rangle + \sin(2K + 1)\theta_0|S\rangle.$$

Si θ_0 est assez petit, (ce qui sera le cas en pratique car $M \ll N$) et si M est connu, on peut choisir le nombre d'itérations K tel que $(2K + 1)\theta_0 \approx \frac{\pi}{2}$ pour obtenir un état final presque parallèle à $|S\rangle$. Une mesure donnera alors une solution avec probabilité proche de 1. Cette analyse est présentée dans le prochain paragraphe.

Revenons maintenant à l'implémentation de la réflexion autour de $|\psi_0\rangle$ dans le circuit quantique. La réflexion d'un vecteur \vec{V} par rapport à $\vec{\psi}_0$ correspond à l'opération suivante (vérifiez le avec un dessin !)

$$\vec{V} \mapsto 2(\vec{\psi}_0^T \cdot \vec{V})\vec{\psi}_0 - \vec{V}.$$

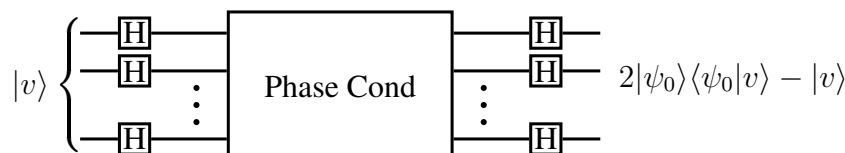
En notation de Dirac :

$$\begin{aligned} |V\rangle &\mapsto 2|\psi_0\rangle\langle\psi_0|V\rangle - |V\rangle \\ &= (2|\psi_0\rangle\langle\psi_0| - I)|V\rangle \\ &= H^{\otimes n}(2|0\dots 0\rangle\langle 0\dots 0| - I)H^{\otimes n}|V\rangle. \end{aligned}$$

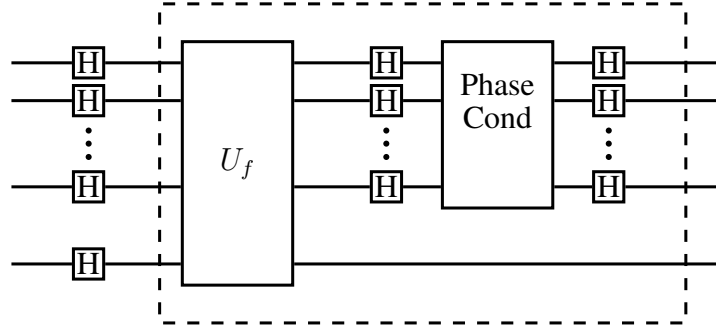
L'opération (unitaire) dans les parenthèses a pour effet de changer la phase des entrées non nulles :

$$(2|0\dots 0\rangle\langle 0\dots 0| - I)|\underline{x}\rangle = \begin{cases} |0\dots 0\rangle & \text{si } \underline{x} = (0\dots 0) \\ -|\underline{x}\rangle & \text{sinon} \end{cases}$$

Nous appelons cet opérateur *Phase Cond* pour *phase conditionnelle*. Le circuit implémentant la réflexion par rapport à $|\psi_0\rangle$ est



En combinant ce circuit avec celui de la figure 1 nous obtenons :



La boîte encadrée représente l'opérateur de Grover appelé G . Son effet sur

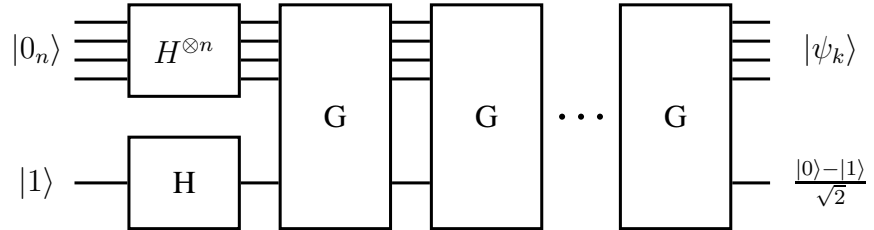
$$\frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = (\cos \theta_0 |P\rangle + \sin \theta_0 |S\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

est d'effectuer une rotation d'angle $2\theta_0$ dans le plan $\{|P\rangle, |S\rangle\}$. La sortie est

$$(\cos 3\theta_0 |P\rangle + \sin 3\theta_0 |S\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

L'algorithme de Grover consiste à itérer cette opération G un certain nombre de fois.

La figure ci-dessous représente le circuit de l'algorithme de Grover :



La profondeur (temps de calcul) du circuit est $O(K)$ et sa largeur $n + 1$.

7.3 Analyse Probabiliste

Nous faisons une mesure sur les bits du premier registre dans la base computationnelle. La probabilité d'obtenir un état $|\underline{x}^*\rangle$ correspondant à une solution \underline{x}^* est :

$$\sin^2(2K + 1)\theta_0 = |\langle S | \psi_K \rangle|^2.$$

Rappelons qu'ici $\sin \theta_0 = \sqrt{\frac{M}{N}}$ et $\cos \theta_0 = \sqrt{1 - \frac{M}{N}}$.

Discutons d'abord le cas facile $M = \frac{N}{4}$. Dans ce cas $\sin \theta_0 = \frac{1}{2}$ et $\cos \theta_0 = \frac{\sqrt{3}}{2}$ ce qui signifie $\theta_0 = \frac{\pi}{6}$. Au bout d'une itération ($K = 1$) l'état est aligné avec $|S\rangle$ car $3\theta_0 = \frac{\pi}{2}$. Nous trouvons donc 1 solution avec probabilité égale à 1 en une mesure et l'oracle a été consulté 1 fois. Bien sûr ce cas est modérément intéressant car quand il y a $\frac{N}{4}$ solutions on peut en trouver une avec probabilité $\frac{1}{4}$ en posant une question aléatoire à un oracle classique. Ensuite on peut amplifier cette probabilité à $1 - \epsilon$ en répétant l'expérience $O(|\ln \epsilon|)$ fois.

Prenons maintenant le cas $M = 1$. Ce cas est classiquement le plus difficile. Dans ce cas $\sin \theta_0 = \frac{1}{\sqrt{N}}$ et donc l'angle θ_0 est très petit, $\theta_0 \approx \frac{1}{\sqrt{N}}$. Donc

$$\sin^2(2K+1)\theta_0 = \sin^2\left(\frac{2K+1}{\sqrt{N}}\right).$$

Pour $\frac{2K+1}{\sqrt{N}} \approx \frac{\pi}{2}$ cette probabilité est proche de 1. C'est à dire qu'avec $K = \lceil \frac{\pi}{4}\sqrt{N} \rceil$ (partie entière supérieure ou inférieure, c'est égal) la probabilité de succès est proche de 1. On peut voir que cette dernière est $1 - O\left(\frac{1}{N}\right)$.

Cas général avec M général connu.

- $M < \frac{3}{4}N$. Alors $\sin \theta_0 < \frac{\sqrt{3}}{2} \Rightarrow \theta_0 < \frac{\pi}{3}$. Itérons $\lfloor \frac{\pi}{4\theta_0} \rfloor = K$ fois. Puisque $\lfloor \frac{\pi}{4\theta_0} \rfloor = \frac{\pi}{4\theta_0} - \frac{1}{2} + \delta$ avec $|\delta| < \frac{1}{2}$ on a :

$$(2K+1)\theta_0 = \frac{\pi}{2} + 2\delta\theta_0$$

avec $2|\delta|\theta_0 < 2|\delta|\frac{\pi}{3} < \frac{\pi}{3}$. Donc $(2K+1)\theta_0 > \frac{\pi}{2} - \frac{\pi}{3}$ et

$$\sin^2(2K+1)\theta_0 > \sin^2\left(\frac{\pi}{2} - \frac{\pi}{3}\right) = \sin^2\frac{\pi}{6} = \left(\frac{1}{2}\right)^2 = \frac{1}{4}.$$

La probabilité de succès est au moins $\frac{1}{4}$ et peut ensuite être amplifiée comme avant.

- $M > \frac{3}{4}N$. On a une probabilité de succès de $\frac{3}{4}$ simplement grâce à une question classique.

Cas général avec M général inconnu. Si M est inconnu nous ne savons pas combien de fois itérer et le problème serait que nous itérons pas assez ou trop. L'algorithme suivant à une probabilité de succès de $\frac{1}{4}$ (ce qui nous suffit car celle-ci peut ensuite être amplifiée).

- 1) Prendre une entrée \underline{x} aléatoirement uniformément. Si $f(\underline{x}) = 1 \rightarrow$ SUCCES

2) Sinon choisir $R \in \{0, 1, 2, \dots, \sqrt{N} - 1\}$ uniformément aléatoirement et appliquer Grover avec R itérations. Mesurer la sortie.

Montrons que la probabilité de succès est toujours $\geq \frac{1}{4}$. Si $M \geq \frac{3}{4}N$ le point 1 à une probabilité de succès $\frac{3}{4}$ qui est plus grand que $\frac{1}{4}$. Si $M < \frac{3}{4}N$ on a sûrement

$$\text{Prob}(\text{succès}) \geq \text{Prob}(\text{succès au point 2}).$$

Mais

$$\begin{aligned} \text{Prob}(\text{succès au point 2}) &= \sum_{R=1}^{\sqrt{N}-1} \text{Prob}(\text{succès au point 2} \mid R) \text{Prob}(R) \\ &= \frac{1}{\sqrt{N}} \sum_{R=0}^{\sqrt{N}-1} \sin^2(2R+1)\theta_0 \\ &= \frac{1}{2} - \frac{\sin 4\sqrt{N}\theta_0}{4\sqrt{N} \sin 2\theta_0}. \end{aligned}$$

La dernière égalité se démontre en représentant le sinus avec des exponentielles complexes (formule d'Euler) puis en utilisant la formule de la somme géométrique. Montrons que cette dernière expression est $\geq \frac{1}{4}$ (pour $M < \frac{3}{4}N$). D'une part $\sin 4\sqrt{N}\theta_0 < 1$. D'autre part

$$\sin 2\theta_0 = 2 \sin \theta_0 \cos \theta_0 = 2\sqrt{\frac{M}{N}} \sqrt{\frac{N-M}{M}} > 2\sqrt{\frac{M}{N}} \sqrt{\frac{N}{4N}} > \frac{1}{\sqrt{N}}.$$

Ces deux remarques impliquent

$$\frac{\sin 4\sqrt{N}\theta_0}{4\sqrt{N} \sin 2\theta_0} \leq \frac{1}{4}$$

d'où

$$\text{Prob}(\text{succès au point 2}) \geq \frac{1}{2} - \frac{1}{4} = \frac{1}{4}.$$

Nous sommes donc assurés d'avoir $\text{Prob}(\text{succès}) \geq \frac{1}{4}$ lors d'une expérience (qui peut ensuite être amplifiée).