EMINES TD3: Algorithme de Grover

Zaki Leghtas*

Janvier 2026

1 Algoirthme de Grover

L'algorithme de Grover est l'un des algorithmes quantiques les plus importants. Il a été découvert par Lov Grover en 1996. Il vise à rechercher des entrées dans une base de données non structurée. Il repose sur des appels multiples d'une fonction oracle. De manière plus générale, l'algorithme de Grover peut être compris comme cherchant à trouver $x \in \{0,1\}^n$ tel que

$$f(x) = 1$$

pour une fonction arbitraire $f : \{0,1\}^n \to \{0,1\}$. Nous allons voir quelle est la nature de l'avantage donné par le parallélisme quantique par rapport au calcul classique.

1. Combien d'appels à l'oracle nécessiterait un algorithme de recherche classique pour effectuer une recherche dans une base de données non structurée ?
   Dans le cas général où f n'a aucune structure, il faut tester les x les uns après les autres. En moyenne, il faut appeler l'oracle $2^n/2$ fois, mais dans le pire des cas, ça peut aller jusqu'à 2^n.

2 Blocks de base

L'algorithme commence par appliquer, sur un registre de n-qubits initialisés en $|0\rangle^{\otimes n}$, une porte de Hadamard sur chaque qubit $\hat{H}^{\otimes n}$. L'algorithme de Grover est composé de trois blocs, qui sont schématisés dans la figure 1 :

- L'oracle unitaire qui appelle la fonction f définie de telle sorte que $f(x) = 1$ pour $x = m$ et $f(x) = 0$ sinon :
  $$\hat{O}_f |k\rangle = (-1)^{f(k)} |k\rangle$$
  où le ket $|k\rangle = |k_0\rangle \otimes |k_1\rangle \otimes \ldots \otimes |k_{n-1}\rangle$ avec $k_0 k_1 \ldots k_{n-1}$ l'écriture binaire de k.
- Une réflexion d'axe $|0\rangle = |0\rangle^{\otimes n}$:
  $$\hat{R} = 2 |0\rangle^{\otimes n} \langle 0|^{\otimes n} - \hat{I}$$
- La porte de Hadamard $\hat{H}^{\otimes n}$.

*zaki.leghtas@ens.fr

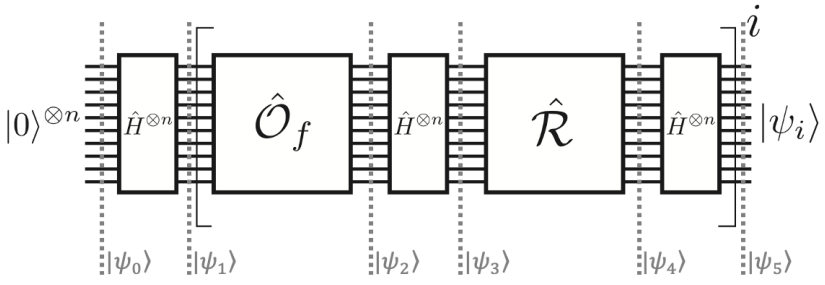

Figure 1: Alogrithme de Grover.

3 Questions

2. Vérifiez que les blocks de base sont bien unitaires.
   $\hat{O}_f$ est diagonal réel dans la base des $|k\rangle$, il est donc hermitien: $\hat{O}_f^\dagger = \hat{O}_f$. On a donc pour tout $|k\rangle$: $\hat{O}_f^\dagger \hat{O}_f |k\rangle = \left((-1)^{f(k)}\right)^2 |k\rangle = |k\rangle$. Donc $\hat{O}_f^\dagger \hat{O}_f = \hat{I}$. Ainsi $\hat{O}_f$ est unitaire.

$$\begin{aligned}\hat{R}^\dagger \hat{R} &= \left(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - \hat{I}\right) \times \left(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - \hat{I}\right) \\ &= 4|0\rangle^{\otimes n}\langle 0| - 2|0\rangle^{\otimes n}\langle 0| - 2|0\rangle^{\otimes n}\langle 0| + \hat{I} \\ &= \hat{I}\end{aligned}$$

   $\left(\hat{H}^{\otimes n}\right)^\dagger \times \hat{H}^{\otimes n} = \left(\hat{H}^\dagger \hat{H}\right)^{\otimes n} = \hat{I}$

3. Montrez que $\hat{H}^{\otimes n}|m\rangle = \frac{1}{\sqrt{N}} \sum_{k=\{0,1\}^n} (-1)^{k.m} |k\rangle$, où $k.m$ est le produit scalaire des écritures binaires ($k.m = \sum k_i m_i$), et $N = 2^n$. Nous introduisons le ket suivant:

$$|\gamma\rangle = \hat{H}^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_{k=\{0,1\}^n} |k\rangle$$

$$\begin{aligned}\hat{H}^{\otimes n}|m\rangle &= \hat{H}^{\otimes n}|m_1\rangle \otimes \cdots \otimes |m_n\rangle \\ &= \hat{H}|m_1\rangle \otimes \cdots \otimes \hat{H}|m_n\rangle \\ &= \frac{1}{2^{n/2}} \left(|0\rangle + (-1)^{m_1}\right) \otimes \cdots \otimes \left(|0\rangle + (-1)^{m_n}\right) \\ &= \frac{1}{2^{n/2}} \left(|00\ldots0\rangle + (-1)^{m_1}|10\ldots0\rangle + (-1)^{m_1+m_2}|11\ldots0\rangle + \ldots\right) \\ &= \frac{1}{2^{n/2}} \left(\sum_k (-1)^{k.m}|k\rangle\right)\end{aligned}$$

4. Exprimez $|\psi_0\rangle$ et $|\psi_1\rangle$ et montrez que $|\psi_2\rangle = |\gamma\rangle - \frac{2}{\sqrt{N}}|m\rangle$.
   $|\psi_0\rangle = |0\rangle^{\otimes n}$
   $|\psi_1\rangle = 2^{-n/2} \sum_{k\in\{0,1\}^n} |k\rangle = |\gamma\rangle$

$$\begin{aligned}|\psi_2\rangle &= \hat{O}_f|\psi_1\rangle \\ &= 2^{-n/2}\hat{O}_f \sum_{k\in\{0,1\}^n} \hat{O}_f|k\rangle \\ &= 2^{-n/2}\left(\sum_{k\neq m} \hat{O}_f|k\rangle + \hat{O}_f|m\rangle\right) \\ &= 2^{-n/2}\left(\sum_{k\neq m} (-1)^{f(k)}|k\rangle + (-1)^{f(m)}|m\rangle\right) \\ &= 2^{-n/2}\left(\sum_{k\neq m} |k\rangle - |m\rangle\right) \\ &= 2^{-n/2}\left(\sum_k |k\rangle - 2|m\rangle\right) \\ &= |\gamma\rangle - \frac{2}{\sqrt{N}}|m\rangle\end{aligned}$$

5. Calculez $|\psi_5\rangle$. Vérifiez que cet état est bien normalisé.
Notez que $\hat{H}^{\otimes n}\hat{R}\hat{H}^{\otimes n} = 2\,|\gamma\rangle\langle\gamma| - \hat{I}$ et donc

$$\begin{aligned}
|\psi_5\rangle &= \left(2\,|\gamma\rangle\langle\gamma| - \hat{I}\right)|\psi_2\rangle \\
&= \left(2\,|\gamma\rangle\langle\gamma| - \hat{I}\right)\left(|\gamma\rangle - \frac{2}{\sqrt{N}}|m\rangle\right) \\
&= \left(1 - \frac{4}{\sqrt{N}}\langle\gamma|m\rangle\right)|\gamma\rangle + \frac{2}{\sqrt{N}}|m\rangle \\
&= \left(1 - \frac{4}{N}\right)|\gamma\rangle + \frac{2}{\sqrt{N}}|m\rangle
\end{aligned}$$

Notez que

$$\begin{aligned}
\langle\psi_5|\psi_5\rangle &= \left(1 - \frac{4}{N}\right)^2 + \frac{4}{N} + 2\left(1 - \frac{4}{N}\right)\frac{2}{\sqrt{N}}\langle\gamma|m\rangle \\
&= \left(1 - \frac{4}{N}\right)^2 + \frac{4}{N} + \left(1 - \frac{4}{N}\right)\frac{4}{N} \\
&= 1
\end{aligned}$$

6. Justifiez que dans la limite où $N \to +\infty$, $|\psi_5\rangle$ peut être écrit sous la forme $|\psi_5\rangle \approx \cos(\theta)\,|\gamma\rangle + \sin(\theta)\,|m\rangle$. Que vaut θ ?
Cette expression correspond à celle trouvée au premier ordre en θ avec $\theta = 2/\sqrt{N}$

7. Donnez une interprétation géométrique de cette première itération de l'algorithme de Grover.
La concatenation des trois blocs correspond à un unitaire $\hat{U} = \hat{H}^{\otimes n}\hat{R}\hat{H}^{\otimes n}\hat{O}_f$, et nous avons calculé

$$\hat{U}\,|\gamma\rangle \approx \cos(\theta)\,|\gamma\rangle + \sin(\theta)\,|m\rangle \ .$$

De plus nous pouvons aisément calculer:

$$\hat{U}\,|m\rangle \approx -\sin(\theta)\,|\gamma\rangle + \cos(\theta)\,|m\rangle \ .$$

Ainsi, $\hat{U}$ correspond à une rotation d'angle θ dans le plan engendré par $\{|\gamma\rangle, |m\rangle\}$.

8. Calculez la probabilité de mesurer $|m\rangle$ après cette première itération de l'algorithme de Grover.
$p = |\langle m|\psi_5\rangle|^2 = \left|(1 - 4/N)/\sqrt{N} + 2/\sqrt{N}\right|^2 \approx 12/N$

9. Donnez la forme de l'état après k itérations de l'algorithme de Grover.

$$|\psi_k\rangle \approx \cos(k\theta)\,|\gamma\rangle + \sin(k\theta)\,|m\rangle$$

10. Au bout de combien d'itérations avons-nous une probabilité d'ordre 1 de mesurer $|m\rangle$?
$k\theta = \pi/2$, donc $k = \frac{\pi}{4}\sqrt{N}$.

11. Conclure sur l'avantage quantique de l'algorithme de Grover.
On a besoin de l'ordre de $\sqrt{N}$ appels à l'oracle, ce qui est un speed up quadratic par rapport au nombre d'appels N de la fonction en classique.

4 3-SAT

En informatique théorique, le problème "SAT" (satisfiability problem) consiste à trouver les solutions à une équation de la forme $f(x) = 1$, où la fonction $f : x \in \{0,1\}^n \to \{0,1\}$. Plus précisément f prend la forme d'une formule logique. En voici un exemple:

$$f(x_0, x_1, x_2) = (\neg x_0 \vee \neg x_1 \vee \neg x_2) \wedge (x_0 \vee \neg x_1 \vee x_2) \wedge (x_0 \vee x_1 \vee \neg x_2) \wedge (x_0 \vee \neg x_1 \vee \neg x_2) \wedge (\neg x_0 \vee x_1 \vee x_2)$$

où les symboles correspondent à: $\neg$ (NOT), $\vee$ (OR), $\wedge$ (AND).

L'exemple précédent appartient à la classe des problèmes "3-SAT". En effet, la fonction f prend la forme $f(x_0, ..., x_{n-1}) = (\tilde{x}_{i_0} \vee \tilde{x}_{j_0} \vee \tilde{x}_{k_0}) \wedge \cdots \wedge (\tilde{x}_{i_p} \vee \tilde{x}_{j_p} \vee \tilde{x}_{j_p})$, et le symbole $\tilde{x}_i$ correspond à x_i ou $\neg x_i$ selon les cas. La classe des problèmes 3-SAT est NP complet, c'est à dire que tout problème NP (vérifiable en temps polynomial) peut être traduit en un problème 3-SAT en temps polynomial.

12. Remplissez le tableau de vérité de la fonction f.

x_0	x_1	x_2	$f(x_0, x_1, x_2)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

13. Montrez que le circuit de la Figure. 2 implémente l'oracle de Grover pour f.
On vérifie que ce circuit implémente un unitaire $\hat{U}$ tel que $\hat{U}|q_0 q_1 q_2\rangle = \pm|q_0 q_1 q_2\rangle$. La dépendence du signe en fonction de q_0, q_1, q_2 est donnée dans le tableau ci-dessous:

q_0	q_1	q_2	signe
0	0	0	+
0	0	1	−
0	1	0	−
0	1	1	−
1	0	0	−
1	0	1	+
1	1	0	+
1	1	1	−

On a donc $\hat{U} = -\hat{O}_f$ (le signe global n'a aucun impact).

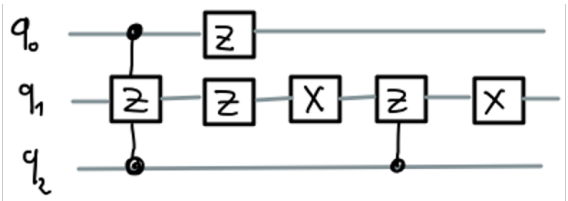

Figure 2: Circuit implémentant l'oracle correspondant à la fonction f.

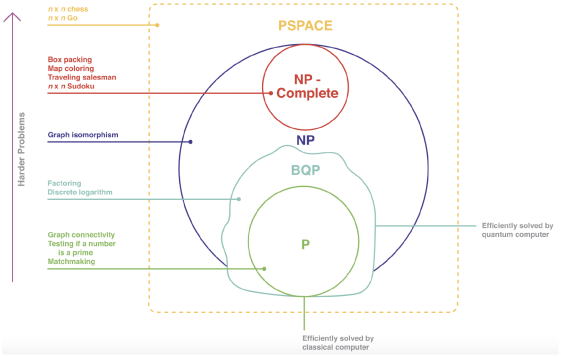

Figure 3: Diagramme de classes de complexité. Extrait de Scott Aaronson: https://www.simonsfoundation.org/report2017/stories/scott-aaronson-quantum-and-classical- uncertainty/