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 l'inversion d'une fonction donnée $f(x)$. Quel entier x satisfait $f(x) = 1$ pour $f : \{0,1\}^n \to \{0,1\}$? 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 ?

2 Blocks de base

L'algorithme commence par appliquer, sur un registre de n-qubits initialisé en $|0\rangle^{\otimes n}$, une porte de Hadamard sur chaque qubit $\hat{H}^{\otimes n}$. L'algorithme de Grover

*zaki.leghtas@ens.fr

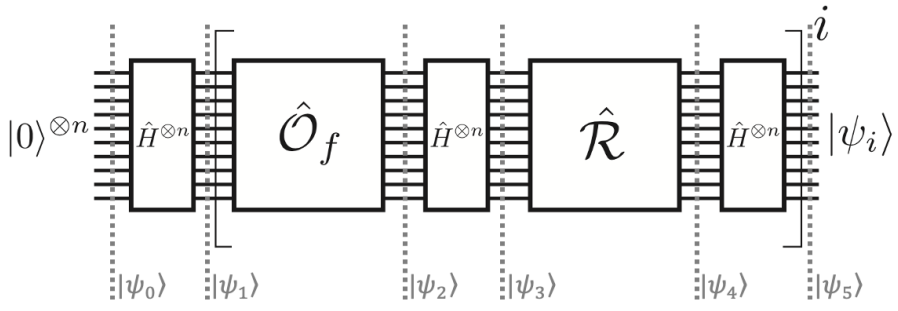

Figure 1: Alogrithme de Grover.

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 :

$$\hat{O}_f \left|k\right\rangle = (-1)^{f(k)} \left|k\right\rangle$$

où le ket $\left|k\right\rangle = \left|k_0\right\rangle \otimes \left|k_1\right\rangle \otimes \ldots \otimes \left|k_{n-1}\right\rangle$ avec $k_0 k_1 \ldots k_{n-1}$ l'écriture binaire de k.

- Une réflexion d'axe $\left|0\right\rangle = \left|0\right\rangle^{\otimes n}$:

$$\hat{R} = 2 \left|0\right\rangle^{\otimes n} \left\langle 0\right|^{\otimes n} - \hat{I}$$

- La porte de Hadamard $\hat{H}^{\otimes n}$.

3 Questions

2. Vérifiez que les blocks de base sont bien unitaires.
3. Montrez que $\hat{H}^{\otimes n} \left|m\right\rangle = \frac{1}{\sqrt{N}} \sum_{k=\{0,1\}^n} (-1)^{k.m} \left|k\right\rangle$, 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:

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

4. Exprimez $\left|\psi_0\right\rangle$ et $\left|\psi_1\right\rangle$ et montrez que $\left|\psi_2\right\rangle = \left|\gamma\right\rangle - \frac{2}{\sqrt{N}} \left|m\right\rangle$.
5. Calculez $\left|\psi_3\right\rangle$.
6. Calculez $\left|\psi_4\right\rangle$.
7. Calculez $\left|\psi_5\right\rangle$. Vérifiez que cet état est bien normalisé.
8. Justifiez que dans la limite où $N \to +\infty$, $\left|\psi_5\right\rangle$ peut être écrit sous la forme $\left|\psi_5\right\rangle \approx \cos(\theta) \left|\gamma\right\rangle + \sin(\theta) \left|m\right\rangle$. Que vaut θ ?
9. Donnez une interprétation géométrique de cette première itération de l'algorithme de Grover.
10. Calculez la probabilité de mesurer $\left|m\right\rangle$ après cette première itération de l'algorithme de Grover.
11. Donnez la forme de l'état après k itérations de l'algorithme de Grover.
12. Au bout de combien d'itérations avons-nous une probabilité d'ordre 1 de mesurer $\left|m\right\rangle$?
13. Conclure sur l'avantage quantique de l'algorithme de Grover.

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.

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

15. Montrez que le circuit de la Figure. 2 implémente l'oracle de Grover pour f.

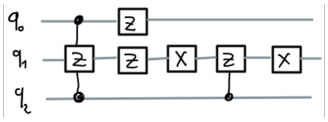

Figure 2: Circuit implémentant l'oracle correspondant à la fonction f.

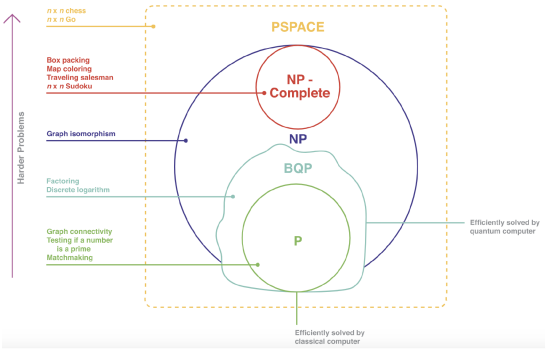

Figure 3: Diagramme de classes de complexité. Extrait de Scott Aaronson: https://www.simonsfoundation.org/report2017/stories/scott-aaronson-quantum-and-classical- uncertainty/