

Informatique Quantique

Frédéric Magniez

Cours 3: Algorithme de Grover Applications et limitations

Problème de recherche abstrait

2

Entrée

- Ensemble $X = \{a, b, c, \dots\}$
- Elements marqués : M sous-ensemble de X

Sortie

- Un élément marqué x de M

Modèle de requêtes

- Coût l pour répondre à “ x dans M ?”

Recherche exhaustive

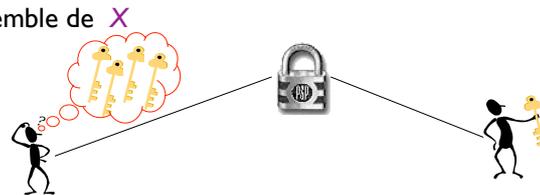
- Trouve un élément marqué en $|X|$ requêtes

Recherche aléatoire

- Trouve un élément marqué en utilisant l/ϵ requêtes $\epsilon = \Pr(M)$

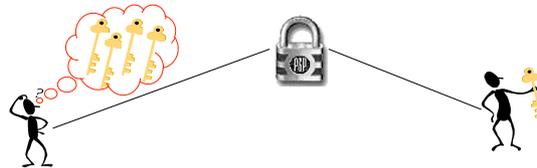
Recherche quantique [Grover, ...]

- Accélération quadratique de la recherche aléatoire
- Trouve un élément marqué en utilisant $l/\sqrt{\epsilon}$ requêtes



Problème revu

- Entrée : $f : \{0, 1\}^n \rightarrow \{0, 1\}$ telle que $\exists! x_0 : f(x_0) = 1$
- Sortie : x_0
- Contrainte : f est une boîte noire



Reformulation

- $N = 2^n$ et $f : \{1, 2, \dots, N\} \rightarrow \{0, 1\}$

Complexité en requêtes

- Probabiliste : $\Theta(N)$
 - Quantique : $\Theta(\sqrt{N})$
- $N = 4 \implies 1$ requête

Implémentation de f

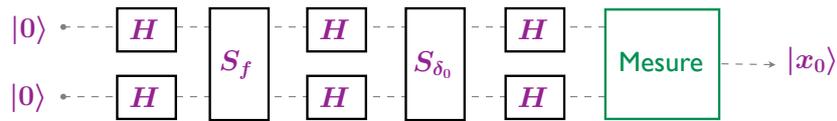
$$\sum_x \alpha_x |x\rangle \xrightarrow{S_f} \sum_x (-1)^{f(x)} \alpha_x |x\rangle = \sum_x \alpha_x |x\rangle - 2\alpha_{x_0} |x_0\rangle$$

Double porte de Hadamard

$$\begin{aligned} |x_1\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle) \\ |x_2\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle) \end{aligned}$$

$$|x\rangle = |x_1 x_2\rangle \xrightarrow{H \otimes H} \frac{1}{2} \sum_y (-1)^{x \cdot y} |y\rangle$$

avec $x \cdot y = x_1 y_1 + x_2 y_2 \pmod 2$



Initialisation : $|00\rangle$

Parallélisation : $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Appel de f : $\frac{1}{2} \sum_x |x\rangle - |x_0\rangle$

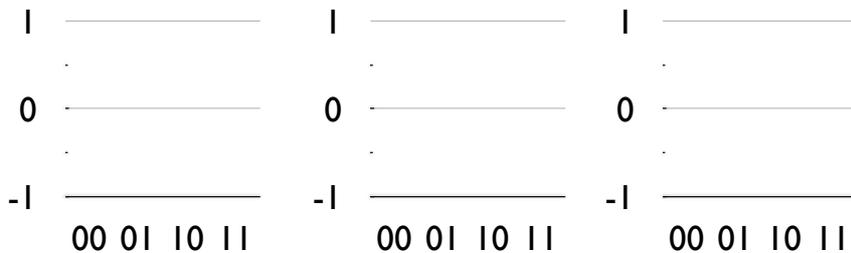
Interférences : $|00\rangle - \frac{1}{2} \sum_y (-1)^{x_0 \cdot y} |y\rangle$

Appel de δ_0 : $-|00\rangle - \frac{1}{2} \left(\sum_y (-1)^{x_0 \cdot y} |y\rangle - 2|00\rangle \right) = -H \otimes H |x_0\rangle$

Regroupement : $-|x_0\rangle$

Opérateur de diffusion

- Soit l'opérateur $D = H^{\otimes 2}(S_{\delta_0})H^{\otimes 2}$. Calculer D
- Montrer que $(-D)$ appliqué à un état $|\psi\rangle$, effectue sur chaque coordonnée une symétrie par rapport à la moyenne des amplitudes.
- A l'aide d'un graphique des amplitudes, représenter le graphe des amplitudes de l'état du circuit après la parallélisation, l'appel de f , puis l'application de $(-D)$



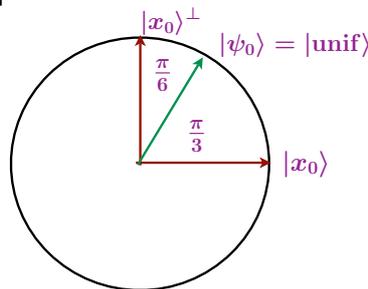
- Montrer que remplacer D par $(-D)$ ne change rien à l'analyse. Conclure
- Justifier pourquoi l'algorithme utilise D

Opérateur de Grover

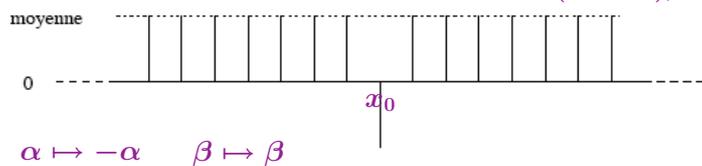


Exercice

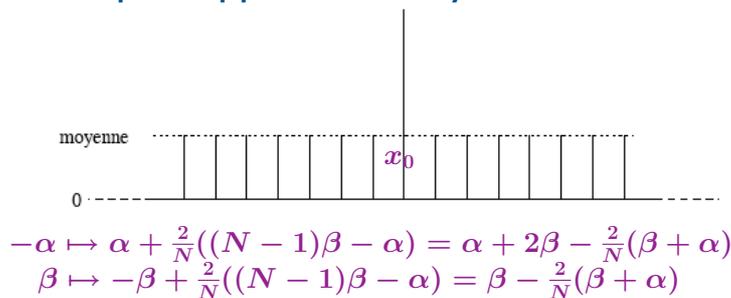
- Pourquoi remplacer S_{δ_0} par $-S_{\delta_0}$ ne change rien à l'analyse ?
- Interpréter S_f comme une symétrie orthogonale dont on calculera l'espace de symétrie.
- Faire de même avec $-S_{\delta_0}$ puis avec $H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2}$
- Montrer que le plan $\text{Vect}_{\mathbb{R}}(|x_0\rangle, |\text{unif}\rangle)$ est stable par G
- Dans ce plan, montrer que G est une rotation dont on calculera l'angle
- Conclure



Changement de phase α : amplitude de x_0 β : autres amplitudes
 $\alpha^2 + (N - 1)\beta^2 = 1$



Inversion par rapport à la moyenne



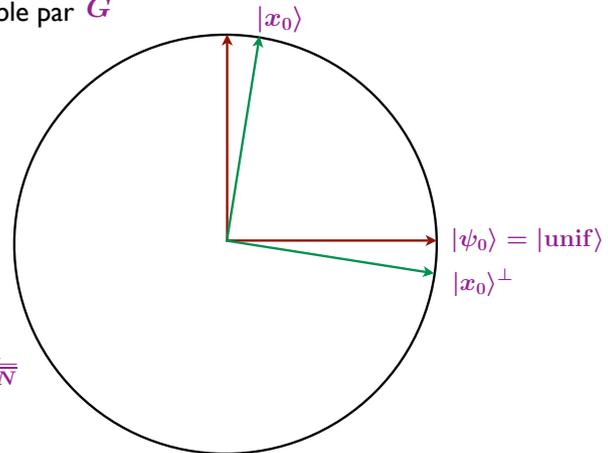
Conclusion : $\alpha_j = \sin((2j + 1)\theta)$ $\sin \theta = \frac{1}{\sqrt{N}}$

- Nombre d'itérations : $T \simeq \frac{\pi}{4}\sqrt{N}$

Opérateur de Grover

$$\cdots \boxed{G} \cdots \stackrel{\text{def}}{=} \cdots \boxed{S_f} \boxed{H} \boxed{-S_{\delta_0}} \boxed{H} \cdots$$

- $\text{Vect}_{\mathbb{R}}(|x_0\rangle, |\text{unif}\rangle)$ est stable par G
- Dans ce plan on a
 - $S_f = -S_{|x_0\rangle} = S_{|x_0\rangle^\perp}$
 - $-S_{\delta_0} = S_{|0^n\rangle}$
 - $H^{\otimes n} S_{|0^n\rangle} H^{\otimes n} = S_{|\text{unif}\rangle}$



Conclusion

- $G = S_{|\text{unif}\rangle} S_{|x_0\rangle^\perp} = R_{2\theta}$
avec $\sin \theta = \langle \text{unif} | x_0 \rangle = \frac{1}{\sqrt{N}}$
- Et donc nombre d'itérations :

$$T \simeq \frac{\pi}{4} \sqrt{N}$$

Optimalité de l'algorithme de Grover

Modélisation

- Soit U un circuit qui résout le problème de Grover avec précision ε

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

- Soit $|\psi_t^i\rangle$ l'état du circuit après la t -ème question à f_i , où

$$f_i : \{1, 2, \dots, N\} \rightarrow \{0, 1\}, x \mapsto \begin{cases} 1, & x = i \\ 0, & x \neq i \end{cases} \quad i = 1, \dots, N$$

$$f_0 \equiv 0$$

- La réponse est soit la solution i soit "pas de solution", cas f_0 . Il faut donc adapter l'algorithme de Grover en vérifiant à la fin que la solution donnée est correcte

Mesure du progrès

$$W_t = \sum_{i=1}^N |\langle \psi_t^0 | \psi_t^i \rangle|^2$$

Condition initiale

$$W_0 = N$$

Condition finale

- Les états finaux $|\psi_T^0\rangle$ et $|\psi_T^i\rangle$ sont quasi-orthogonaux :
 $|\langle \psi_T^0 | \psi_T^i \rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)} \implies |W_T| \leq 2N\sqrt{\varepsilon(1-\varepsilon)}$

Majoration des sauts

Exercice : Vérifier cette majoration

- Les applications unitaires ne comptent pas :

$$\langle \psi_t^0 | \psi_t^i \rangle = \langle \psi_t^0 U | U \psi_t^i \rangle$$

- Influence des questions.

$$\begin{aligned} |\langle \psi_t^0 | \psi_t^i \rangle - \langle \psi_{t+1}^0 | \psi_{t+1}^i \rangle| &= |\langle \psi_t^0 | \psi_t^i \rangle - \langle \psi_t^0 U_{f_i} | \psi_t^i \rangle| \\ &\leq |\langle \psi_t^0 | P_i | \psi_t^i \rangle| + |\langle \psi_t^0 | P_i U_{f_i} | \psi_t^i \rangle| \\ &\leq 2\|P_i | \psi_t^0 \rangle\| \end{aligned}$$

Exercice : Vérifier cette majoration

- Au total :

$$|W_t - W_{t+1}| \leq \sum_{i=1}^N 2\|P_i | \psi_t^0 \rangle\| \leq 2\sqrt{N} \sqrt{\sum_{i=1}^N \|P_i | \psi_t^0 \rangle\|^2} = 2\sqrt{N}$$

Conclusion

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

Cas des solutions multiples

Nombre connu : t

$$\sin \theta = \langle \text{unif} | \frac{1}{\sqrt{k}} \sum_{x_0} |x_0\rangle = \sqrt{\frac{t}{N}} \implies \frac{\pi}{4} \sqrt{\frac{N}{t}} \text{ itérations conviennent}$$

Nombre inconnu (I) : réduction probabiliste

- Partir de $m = 1$
- Choisir aléatoirement un entier $j \in \{0, 1, \dots, m-1\}$
- Effectuer j itérations de l'opérateur de Grover sur la superposition uniforme $\frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle$
- Observer le registre, soit i la sortie obtenue
- Si $F(i) = 1$, alors renvoyer i et s'arrêter
- Sinon, fixer $m = \min(8m/7, \sqrt{N})$ et recommencer

Théorème : temps moyen = $O(\sqrt{\frac{N}{t}})$

Nombre inconnu (II) : comptage quantique

- Temps (dans tous les cas) : $O(\sqrt{\frac{N}{t}})$

Etat initial (obtenu par un circuit quantique)

$$A : |0\rangle \mapsto |p\rangle = \sum \sqrt{p_x} |x\rangle$$

Opérateur de requêtes

$$O_M : |x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } x \in M \\ |x\rangle & \text{otherwise} \end{cases}$$

Etat recherché

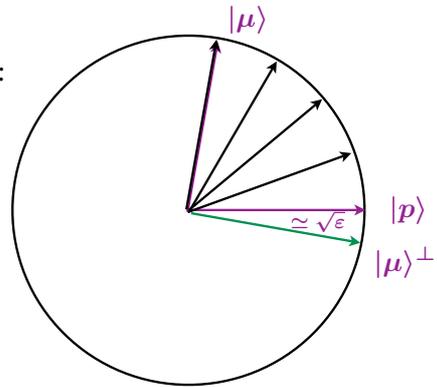
- Projection de $|p\rangle$ sur $\text{span}(|x\rangle : x \in M)$:

$$|\mu\rangle = \frac{1}{\sqrt{\varepsilon}} \sum_{x \in M} \sqrt{p_x} |x\rangle$$

- Probabilité de succès initiale $|\langle \mu | p \rangle|^2 = \varepsilon$

Symétries dans $\text{span}(|p\rangle, |\mu\rangle)$

- O_M : symétrie selon $|\mu\rangle^\perp$
- $A(-O_0)A^{-1}$: symétrie selon $|p\rangle$
- **Operator de Grover** : $A(-O_0)A^{-1}O_M$ est une rotation d'angle $\simeq 2\sqrt{\varepsilon}$



Conclusion

- $\frac{\pi}{4\sqrt{\varepsilon}}$ iterations de l'opérateur de Grover sur $|p\rangle$: $\simeq |\mu\rangle$

Exercice 1

- Combien de requêtes sont-elles nécessaires si $t = N/4$?

Exercice 2

- Soit une fonction $f : \{1, \dots, N\} \rightarrow \{1, \dots, N\}$ 2-vers-1

$$\forall x \exists ! y : f(x) = f(y)$$

- Combien de requêtes à f utilisez-vous classiquement pour trouver une paire $(x, y) : x \neq y, f(x) = f(y)$?
- Même question quantiquement.

Exercice 3

- Même exercice sans hypothèse sur f