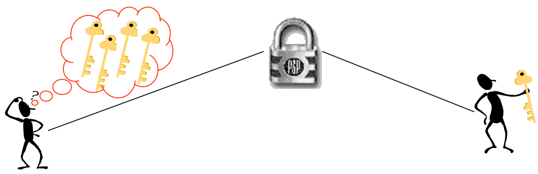
Informatique Quantique

Frédéric Magniez

Cours 3:
Algorithme de Grover
Transformée de Fourier quantique

Problème

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



Reformulation

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

Complexité en requêtes

- Probabiliste : $\Theta(N)$
- Quantique : $\Theta(\sqrt{N})$

$N = 4 \implies 1$ requête

Remarques préliminaires

Implémentation de f

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

Double porte de Hadamard

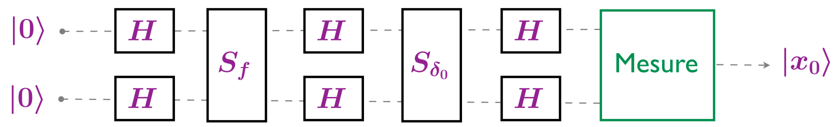
$$|x_1\rangle \xrightarrow{\boxed{H}} \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$$

$$|x_2\rangle \xrightarrow{\boxed{H}} \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)$$

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

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

Solution quantique ($N = 4$)



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 $(-D)$

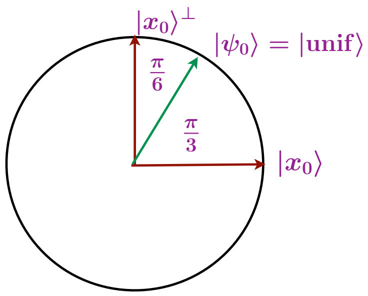
- Montrer que remplacer D par $(-D)$ ne change rien à l'analyse. Conclure
- Justifier pourquoi l'algorithme utilise D

Opérateur de Grover

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

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 $\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle, |\mathrm{unif}\rangle)$ est stable par G
- Dans ce plan, montrer que G est une rotation dont on calculera l'angle
- Conclure

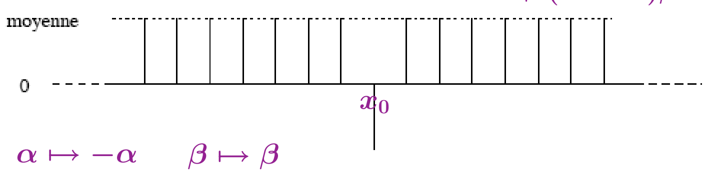


Analyse numérique

Changement de phase

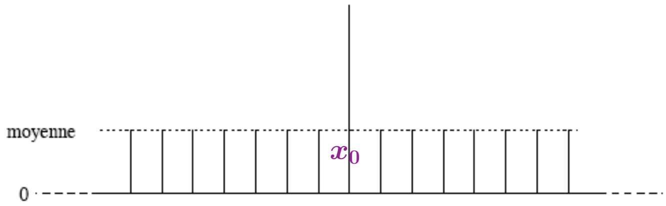
α : amplitude de x_0 $\quad\beta$: autres amplitudes

$$\alpha^2 + (N-1)\beta^2 = 1$$



$\alpha \mapsto -\alpha \qquad \beta \mapsto \beta$

Inversion par rapport à la moyenne



$$-\alpha \mapsto \alpha + \tfrac{2}{N}((N-1)\beta - \alpha) = \alpha + 2\beta - \tfrac{2}{N}(\beta+\alpha)$$
$$\beta \mapsto -\beta + \tfrac{2}{N}((N-1)\beta - \alpha) = \beta - \tfrac{2}{N}(\beta+\alpha)$$

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

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

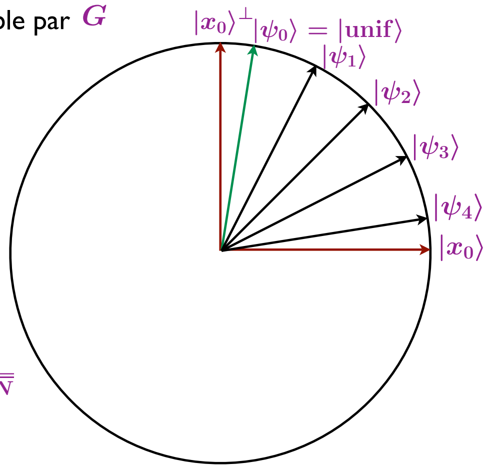
Analyse géométrique

Opérateur de Grover

$$\boxed{G} \overset{\text{def}}{=} \boxed{S_f}\,\boxed{H}\,\boxed{-S_{\delta_0}}\,\boxed{H}$$

- $\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle, |\mathrm{unif}\rangle)$ est stable par G
- Dans ce plan on a

$$S_f = -S_{|x_0\rangle} = S_{|x_0\rangle^\perp}$$
$$-S_{\delta_0} = S_{|0^n\rangle}$$
$$H^{\otimes n} S_{|0^n\rangle} H^{\otimes n} = S_{|\mathrm{unif}\rangle}$$



Conclusion

- $G = S_{|\mathrm{unif}\rangle} S_{|x_0\rangle^\perp} = R_{2\theta}$

  avec $\sin\theta = \langle \mathrm{unif} | x_0 \rangle = \frac{1}{\sqrt{N}}$
- Et donc nombre d'itérations :

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

Cas des solutions multiples

Nombre connu : t

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

Nombre inconnu (I) : réduction probabiliste

- Partir de $m = 1$
- Choisir aléatoirement un entier $j \in \{0, 1, \ldots, m-1\}$
- 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) : $O(\sqrt{\frac{N}{t}})$

Exercices

Exercice 1

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

Exercice 2

- Soit une fonction $f : \{1, \ldots, N\} \to \{1, \ldots, N\}$ 2-vers-1

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

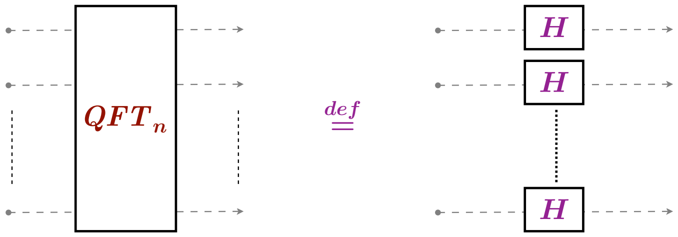
- Combien de requêtes à f utilisez-vous classiquement pour trouver une paire $(x, y) : x \neq y, f(x) = f(y)$?
- Même question quantiquement.

Exercice 3

- Même exercice sans hypothèse sur f

Transformée de Fourier quantique

Rappels



$$QFT_n|x\rangle = \frac{1}{2^{n/2}}\sum_y (-1)^{x\cdot y}|y\rangle$$

avec $x \cdot y = \sum_i x_i y_i \mod 2$

Un peu de théorie...

Transformée de Fourier discrète

- Base de dirac de l'espace des fonctions $f : \{0,1\}^n \to \mathbb{C}$

  $(\delta_x)_{x\in\{0,1\}^n} : f = \sum_{x\in\{0,1\}^n} f(x)\delta_x$

- Base de Fourier de l'espace des fonctions $f : \{0,1\}^n \to \mathbb{C}$

  $(\chi_y)_{y\in\{0,1\}^n}, \chi_y(x) = (-1)^{x\cdot y}$:

  $$\chi_y(x \oplus x') = \chi_y(x)\chi_y(x')$$

  $$f = \frac{1}{2^n}\sum_{y\in\{0,1\}^n} \hat{f}(y)\chi_y,\ \hat{f}(y) = \sum_{x\in\{0,1\}^n} \chi_y(x)f(x)$$

Analogue quantique

- Etat normé $\leftrightarrow$ Fonction normée de L_2

  $$|\psi\rangle = \sum_x \alpha_x|x\rangle \leftrightarrow f : x \mapsto \alpha_x$$

- Circuit quantique de taille n contre $n2^n$ en classique

  $$QFT_n : |x\rangle \mapsto \frac{1}{2^{n/2}}\sum_y (-1)^{x\cdot y}|y\rangle$$

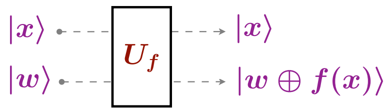
  $$|f\rangle = \sum_x f(x)|x\rangle \mapsto \frac{1}{2^{n/2}}\sum_y \hat{f}(y)|y\rangle$$

Le problème de Simon

Problème

- Entrée : $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ telle que

  $\exists s \in \{0,1\}^n : \forall x \neq y,\ f(x) = f(y) \iff y = x \oplus s$
- Sortie : s
- Contrainte : f est une boîte noire



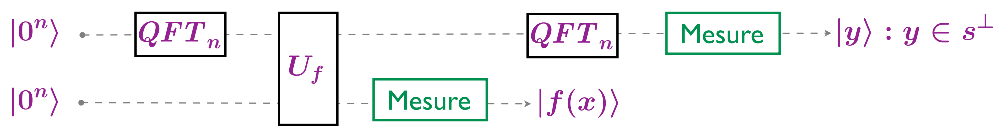
Complexité en requêtes

- Probabiliste : $2^{\Omega(n)}$
- Quantique : $O(n)$

Idée

Utiliser QFT pour rechercher la période s.

Solution quantique



Initialisation : $|0^n\rangle|0^n\rangle$

Parallélisation : $\frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle$

Appel de f : $\frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle$

Mesure partielle : $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle$

Interférences :

$$\frac{1}{2^{(n+1)/2}} \sum_y \left((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}\right)|y\rangle|f(x)\rangle$$

$$\frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x \cdot y}\left(1 + (-1)^{s \cdot y}\right)|y\rangle|f(x)\rangle$$

$$\frac{1}{2^{(n-1)/2}} \sum_{y : s \cdot y = 0} |y\rangle|f(x)\rangle$$

Création du système

- Après $n+k$ itérations : $y_1, y_2, \ldots, y_{n+k} \in s^{\perp}$
- Si $s = 0^n$ les y sont de rang n avec proba $\geq 1 - \frac{1}{2^k}$
- Si $s \neq 0^n$ les y sont de rang $n-1$ avec proba $\geq 1 - \frac{1}{2^{k+1}}$
- Système :

$$\begin{cases} y_1 \cdot t = 0 \\ y_2 \cdot t = 0 \\ \vdots \\ y_{n+k} \cdot t = 0 \end{cases}$$

Solutions du système : 0^n et s !

Temps total : $O(n^3)$

Lemme

- Soient G un groupe fini et H un sous-groupe strict de G, alors

$$\Pr_{x \in G}[x \notin H] \geq \frac{1}{2}$$

Lemme

- Soit G un groupe commutatif fini. Alors G a au plus $|G|$ sous-groupes stricts.

Théorème

- Soit G un groupe commutatif fini, alors

$$\Pr_{x_1, x_2, \ldots, x_l \in G}[\langle x_1, x_2, \ldots, x_l \rangle = G] \geq 1 - \frac{|G|}{2^l}$$

Preuve

- Soit H un sous-groupe strict de G, alors

$$\Pr_{x_1, x_2, \ldots, x_l \in G}[\langle x_1, x_2, \ldots, x_l \rangle \leq H] \leq \frac{1}{2^l}$$

- G a au plus $|G|$ sous-groupes stricts donc

$$\Pr_{x_1, x_2, \ldots, x_l \in G}[\exists H < G : \langle x_1, x_2, \ldots, x_l \rangle \leq H] \leq \frac{|G|}{2^l}$$

Exercice 1 : sous-groupe caché

- Refaire l'algorithme de Simon lorsque
$$f(x) = f(y) \iff y - x \in H$$
où H est un sous-groupe inconnu de $(\{0,1\}^n, \oplus)$
- Montrer la formule $\sum_{h \in H} (-1)^{h \cdot y} = \begin{cases} |H|, & y \in H^\perp \\ 0, & y \notin H^\perp \end{cases}$
- En déduire qu'on peut trouver des générateurs de H en temps $O(n^3)$

Exercice 2 : translation cachée

- Soient deux bijections $f, g : \{0,1\}^n \to \{0,1\}^n$ telles que
$$\exists u \in \{0,1\}^n : \forall x \in \{0,1\}^n,\ f(x) = g(x \oplus u)$$
- Montrer qu'on peut trouver u en temps $O(n^3)$

  Indication : considérer la fonction
$$F(x,b) = \begin{cases} f(x), & b = 0 \\ g(x), & b = 1 \end{cases}$$

Groupe abélien quelconque

- Trouver la période d'une fonction *quelconque* se résout en temps quantique $\mathrm{poly}(\log|G|)$
- Calcul de l'ordre se résoud en temps quantique polynomial

  Entrée : $N, a \in \mathbb{N}$ tels que $\mathrm{pgcd}(a,N) = 1$

  Sortie : le plus petit entier $r \neq 0$ tel que $a^r = 1 \mod N$

Factorisation

- Entrée : $N \in \mathbb{N}$
- Sortie : un diviseur non trivial de N

Réduction : Factorisation $\leq_{\mathrm{R}}$ Calcul de l'ordre

- Vérifier que $\mathrm{pgcd}(a,N) = 1$
- Calculer l'ordre r de $a \mod N$
- Recommencer si r impair ou $a^{r/2} = -1 \mod N$
- Sinon $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \mod N$
- Renvoyer $\mathrm{pgcd}(a^{r/2} \pm 1, N)$