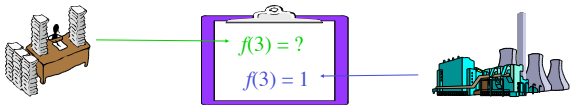
Informatique Quantique

Frédéric Magniez

Cours 3:
Algorithmes élémentaires, algorithme de Grover

Problème

- Entrée : $f : \{0,1\}^n \to \{0,1\}$ soit constante, soit balancée
- Sortie : 0 ssi f est constante
- Contrainte : f est une boîte noire



Complexité en requêtes

- Déterministe : $1 + 2^{n-1}$
- Quantique : 1

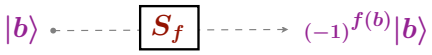
Cas $n = 1$

- Problème équivalent à décider si $f(0) = f(1)$ pour f quelconque

Solution quantique ($n = 1$)

STOP $x \mapsto f(x)$ n'est pas nécessairement réversible !

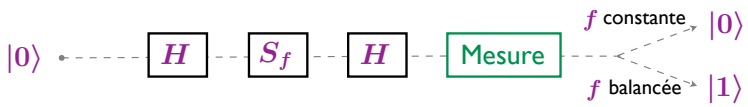
Implémentation de f



Porte de Hadamard : lame demi-onde à 22,5°

Circuit quantique

Analyse ($n = 1$)



Initialisation : $|0\rangle$

Parallélisation : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

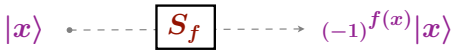
Appel de la fonction : $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

Interférences : $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$

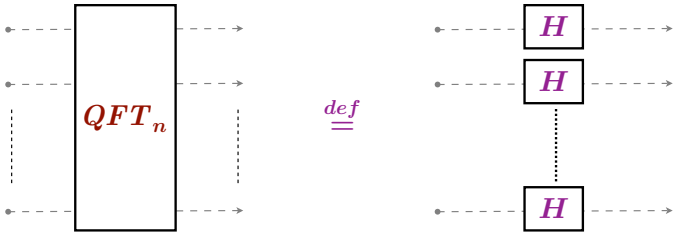
Au final : $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle)$

STOP Dans ce cas la supériorité du quantique ne vient pas de l'enchevêtrement, mais des interférences constructives et destructives.

Implémentation de f



Transformée de Fourier quantique



Exercice

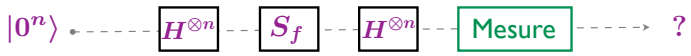
- Vérifier que

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

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

Exercice 1

- Montrer que le circuit suivant résout le problème



Exercice 2

- Montrer que le même circuit permet de trouver f avec la promesse que

$$f(x) = a \cdot x$$

- Remarque : on montre que pour ce problème, la complexité probabiliste en requêtes est en $\Omega(2^{n/2})$

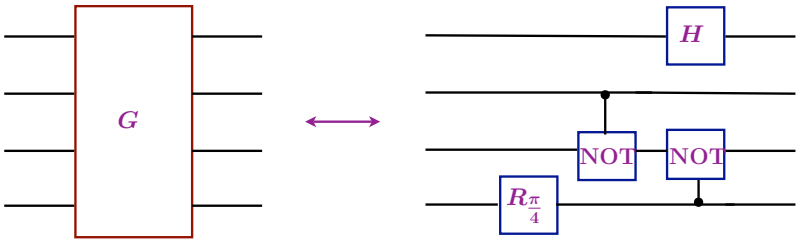
Portes

- Une porte est une transformation unitaire qui agit au plus **3**-qubit

$$U \in \mathcal{U}(2^k), \quad k = 1, 2, 3$$

Circuit

- Un circuit est la décomposition d'une transformation unitaire en portes



$$G = ((I_8 \otimes R_{\frac{\pi}{4}})(I_2 \otimes \text{c-Not})(H \otimes I_2 \otimes \text{c-Not'})$$

Théorème

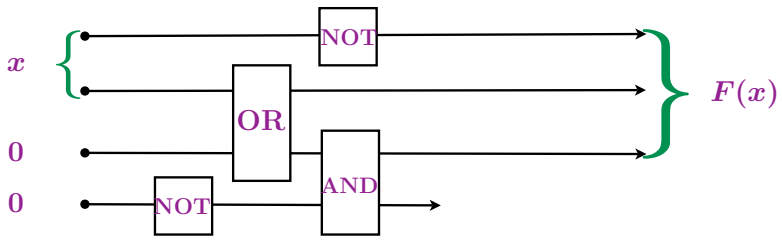
- Il existe une famille universelle finie de portes à 1-qubit et 2-qubit

Définition

- Un circuit $C = C_L \dots C_2 C_1$ calcule une fonction F si pour toute entrée x:

$$C(x, 0^k) = (F(x), z)$$

- La taille d'un circuit est le nombre de portes utilisées pour le réaliser.
- La complexité d'une fonction est la taille minimale du circuit qui la calcule



Remarque

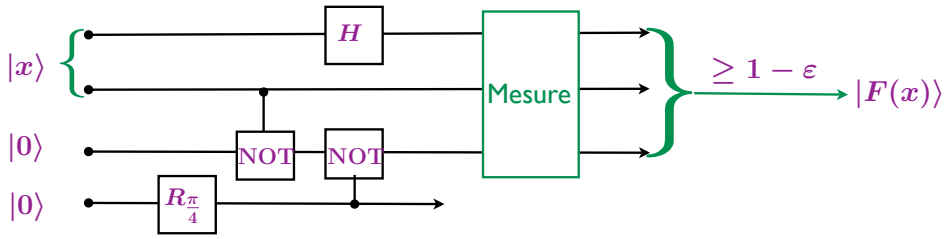
- La complexité d'une fonction ne dépend pas du choix de base universelle de portes (à une constante multiplicative près qui ne dépend que des bases)

Définition

- Un circuit $U = U_L \dots U_2 U_1$ calcule une fonction F avec erreur ε si pour toute entrée x :

$$\sum_z |\langle F(x), z|U|x, 0^k\rangle|^2 \geq 1 - \varepsilon$$

- La taille d'un circuit est le nombre de portes utilisées pour le réaliser.
- La complexité approchée (resp. exacte) d'une fonction est la taille minimale du circuit qui la calcule avec erreur 1/3 (resp. 0)



Remarques

- La complexité d'une fonction ne dépend pas du choix de base universelle
- L'erreur peut arbitrairement être réduite à ε par $\log(1/\varepsilon)$ itérations

Circuit réversible

- Un circuit logique est réversible s'il n'utilise que des portes réversibles
- Un circuit réversible est aussi un circuit quantique
  (car il permute les éléments de la base classique)

Notation : $f : \{0,1\}^n \to \{0,1\}^m$

$$f_\oplus : \{0,1\}^{n+m} \to \{0,1\}^{n+m} \qquad f_\oplus(x,y) = (x, y \oplus f(x))$$

Théorème

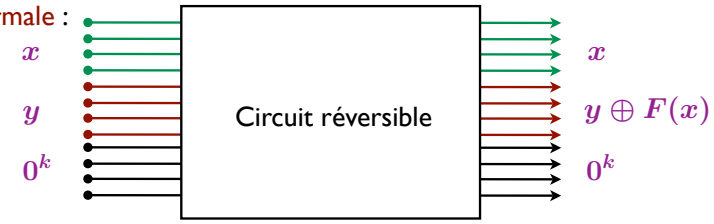
- Toute fonction F calculable par un circuit logique de taille L est aussi calculable par un circuit réversible de taille $O(L)$

  porte f ➡ porte réversible $f_\oplus$ + c-NOT

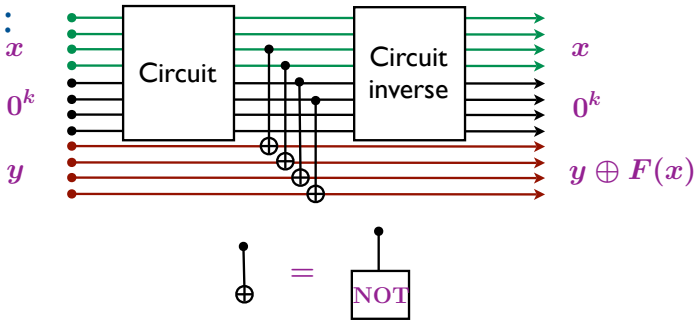
Forme normale d'un calcul réversible

Théorème

- Dans le théorème précédent on peut demander que le circuit calcule $F_\oplus$ et que les bits auxiliaires reviennent à 0, *i.e.* que le circuit soit en forme normale :



Preuve :



Calcul réversible vs calcul quantique

Corollaire

- Si *F* a une complexité classique *L* alors sa complexité quantique est en *O*(*L*)
- *F* et c-*F* ont des complexités classiques (resp. quantiques) équivalentes

Théorème

- La porte de Toffoli (avec la porte NOT pour générer des bits à 1) est universelle pour le calcul réversible

$$T(a,b,c) = (a,b,c \oplus (a \wedge b))$$

- La porte de Toffoli (avec NOT...) et la porte de Hadamard sont universelles pour le calcul quantique
- La porte c-NOT et racine carrée de NOT (ou Hadamard) sont universelles pour le calcul quantique

Exercice

- Montrer comment implémenter $S_F|x\rangle = (-1)^{F(x)}|x\rangle$, lorsque F est à valeurs booléennes, en utilisant $U_F|x,y\rangle = |F_\oplus(x,y)\rangle = |x, y \oplus F(x)\rangle$

Théorème

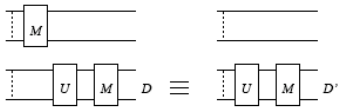
- Une fonction calculable par un circuit avec des mesures intermédiaires l'est aussi par un circuit comparable avec uniquement une mesure à la fin.

Exercice

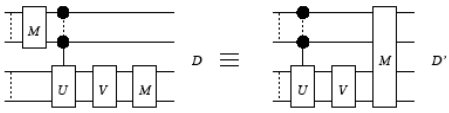
- Montrer le théorème pour les cas suivants :

  Faire un raisonnement à l'aide de matrices densités bien choisies

  Mesure implicite



  Mesure de contrôle



Définition

- Un algorithme quantique pour le calcul d'une fonction $F : \{0,1\}^* \to \{0,1\}^*$ est un algorithme classique qui calcule une famille de circuits $(C_n)_{n\in\mathbb{N}}$ telle que C_n calcule avec précision $\varepsilon > 1/2$ la fonction F restreinte aux entrées de $\{0,1\}^n$
- La complexité en temps $T(n)$ d'un algorithme quantique est la taille du circuit C_n **PLUS** le temps qu'il faut pour décrire le circuit C_n avec précision $O(1/|C_n|)$

Remarques

- En règle générale la description du circuit est négligeable
- Les amplitudes des portes sont donc calculables !
- La complexité *ne dépend pas* du choix des portes

Classes de complexité

- Fonctions (problèmes) calculable (résoluble) en temps polynomial en la taille de l'entrée

  déterministe : P

  probabiliste avec précision $\varepsilon > 1/2$: BPP

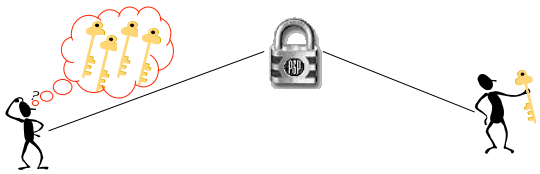
  quantique avec précision $\varepsilon > 1/2$: BQP

$$\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{BQP}$$

Le problème des cadenas

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 : $\Theta(\sqrt{N})$ (preuve de l'optimalité en projet !)

$$N = 4 \implies 1 \text{ requête}$$

Remarques préliminaires

Implémentation de f

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

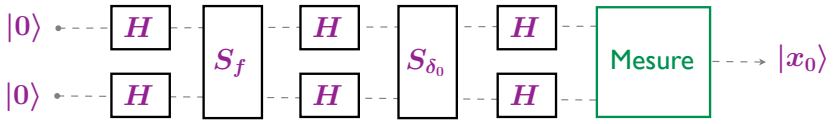
Double porte de Hadamard

$$|x_1\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$$
$$|x_2\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)$$

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

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

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

Regroupement : $-|x_0\rangle$

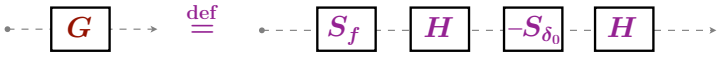
Exercice : Analyse numérique

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 $(-D)$

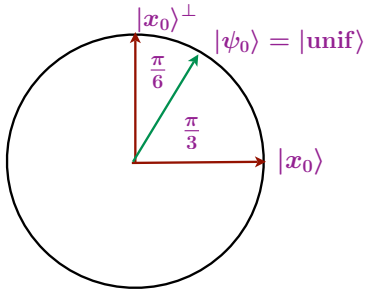
- Montrer que remplacer D par $(-D)$ ne change rien à l'analyse. Conclure
- Justifier pourquoi l'algorithme utilise D

Opérateur de Grover



Exercice

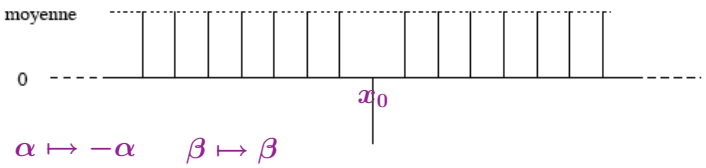
- Pourquoi remplacer S_{δ_0} par $-S_{\delta_0}$ ne change rien à l'analyse ?
- Interpréter S_f comme une symétrie orthogonale dont on calculera l'espace de symétrie.
- Faire de même avec $-S_{\delta_0}$ puis avec $H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2}$
- Montrer que le plan $\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle,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



Changement de phase

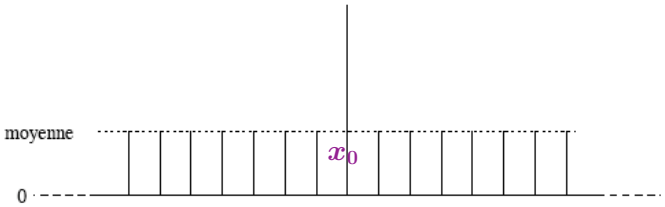
α : amplitude de x_0 β : autres amplitudes

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



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

Inversion par rapport à la moyenne



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

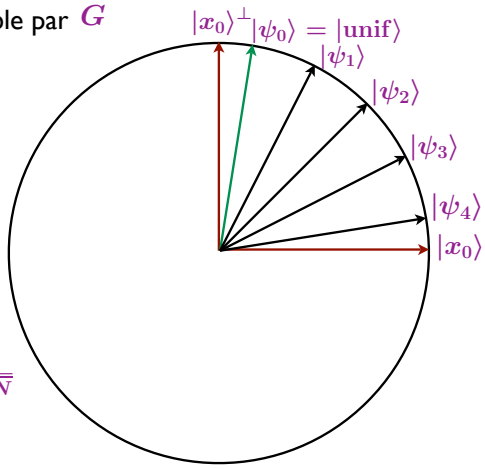
Conclusion : $\alpha_j = \sin((2j+1)\theta)$ $\sin\theta = \frac{1}{\sqrt{N}}$

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

Opérateur de Grover

- $\mathrm{Vect}_{\mathbb{R}}(|x_0\rangle, |\mathrm{unif}\rangle)$ 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 :

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

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) : $O(\sqrt{\frac{N}{t}})$

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