Informatique Quantique

Frédéric Magniez

Cours 5 :
Optimalité de Grover
Transformée de Fourier quantique et applications

Optimalité de l'algorithme de Grover

Modélisation

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

$$U = U_T f_\oplus \dots U_2 f_\oplus U_1 f_\oplus U_0$$

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

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

$$f_0 \equiv 0$$

- 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

Fonction test

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

Condition initiale

$$W_0 = N$$

Optimalité de l'algorithme de Grover (suite)

Condition finale

- Les états finaux $|\psi_T^0\rangle$ et $|\psi_T^i\rangle$ sont quasi-orthogonaux :

$$|\langle\psi_T^0|\psi_T^i\rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)} \implies W_T \leq 2N\sqrt{\varepsilon(1-\varepsilon)}$$

Exercice :Vérifier cette majoration

Majoration des sauts

- 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.

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

Exercice :Vérifier cette majoration

- Au total :

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

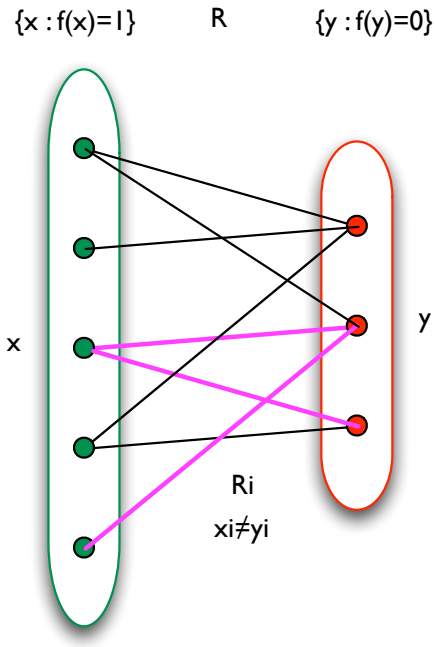
Conclusion

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

Méthode générale

Hypothèses

- Degré gauche de R ≥ m
- Degré droite de ≥ m'
- Degré grauche de tout Ri ≤ l
- Degré droite de tout Ri ≤ l'



Conséquencs

- |R| ≥ m|X|, m'|Y|
- |Ri| ≤ l|X|, l'|Y|

Résultat

$$T = \Omega\left(\sqrt{\frac{mm'}{ll'}}\right)$$

Schéma de la preuve

Etat du système

- étape t, entrée x : $|\psi_t^x\rangle$

Contraintes du modèle de calcul

- FIXONS (x,y) dans R
- Au début : $\langle\psi_0^x|\psi_0^y\rangle = 1$
- A chaque étape : $|\langle\psi_t^x|\psi_t^y\rangle - \langle\psi_{t+1}^x|\psi_{t+1}^y\rangle| \leq 2 \sum_{i:x_i\neq y_i} \sqrt{p_t^x(i)p_t^y(i)}$ (Progress$_{t,x,y}$(i))
- A la fin : $|\langle\psi_T^x|\psi_T^y\rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)}$

$$T \cdot \sum_i 2\sqrt{p_t^x(i)p_t^y(i)} \quad \geq \quad 1-2\sqrt{\varepsilon(1-\varepsilon)}$$

Contraintes combinatoires de la fonction

- Prise en compte de TOUTES les paires (x,y) de R

$$\sum_i Progress_t(i) \leq 2\sqrt{l|X| \cdot l'|Y|}$$

somme de tous les Progress$_{t,x,y}$(i) pour (x,y) de R

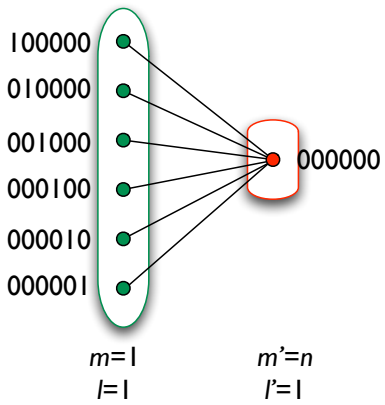
- |R| ≥ m|X|, m'|Y| donc ≥ $\sqrt{mm'|X||Y|}$

Conclusion : $T = \Omega\left(\sqrt{\frac{mm'}{ll'}}\right)$

Exemples

Fonction OR

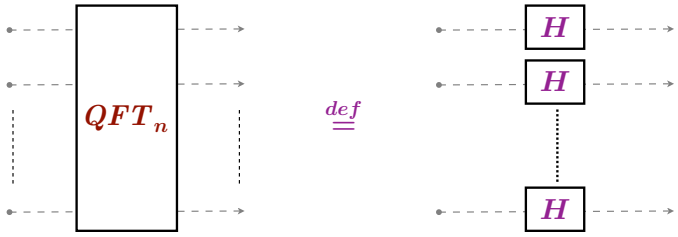
- Complexité quantique $\geq \sqrt{\frac{mm'}{ll'}} = \sqrt{n}$



Exercice

- Complexité de la fonction XOR ?
- Complexité de la fonction Majorité ?

Rappels



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

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

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

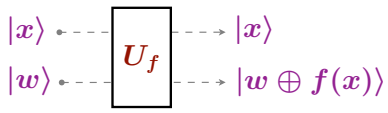
  $QFT_n : |x\rangle \mapsto \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$

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

Le problème de Simon

Problème

- Entrée : $f : \{0,1\}^n \to \{0,1\}^n$ 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



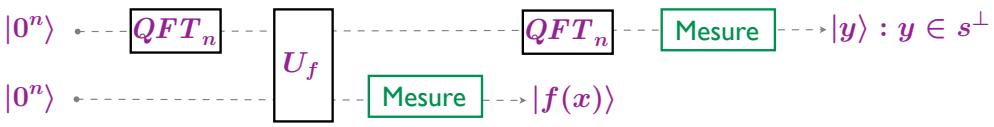
Complexité en requêtes

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

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

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

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 $\mathrm{pgcd}(a^{r/2} \pm 1, N)$

RSA Challenges

- http://www.rsasecurity.com/rsalabs

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	$20,000	Factored	November 2, 2005	F. Bahr et al.
RSA-704	$30,000	Not Factored		
RSA-768	$50,000	Not Factored		
RSA-896	$75,000	Not Factored		
RSA-1024	$100,000	Not Factored		
RSA-1536	$150,000	Not Factored		
RSA-2048	$200,000	Not Factored		

- RSA-640 (193 chiffres) :

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

=

1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579

×

1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

- Algorithme RSA (permet de partagé des secrets)
  difficulté basée sur celle de la factorisation

Transformée de Fourier discrète

- Base de Fourier de l'espace des fonctions $f : \mathbb{Z}_N \to \mathbb{C}$

$$(\chi_y)_{y\in\mathbb{Z}_N}, \chi_y(z) = \omega_N^{xy} \quad \text{avec} \quad \omega_N = e^{2i\pi/N}$$

$$\chi_y(x +_{\mathrm{mod}\, N} x') = \chi_y(x)\chi_y(x')$$

$$f = \frac{1}{N}\sum_{y\in\mathbb{Z}_N} \hat{f}(y)\chi_y,\ \hat{f}(y) = \sum_{x\in\mathbb{Z}_N} \overline{\chi_y(x)} f(x)$$

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 $(\log N)^2$ contre $N \log N$ en classique

$$QFT_{\mathbb{Z}_N} : |x\rangle \mapsto \frac{1}{\sqrt{N}}\sum_y \omega_N^{xy}|y\rangle$$

$$|f\rangle = \sum_x f(x)|x\rangle \mapsto \frac{1}{\sqrt{N}}\sum_y \overline{\hat{f}(y)}|y\rangle$$

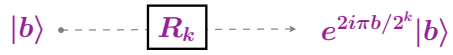
car on n'a pas conjugué ω par commodité

Circuit réalisant la transformée de Fourier sur $\mathbb{Z}_{2^n}$

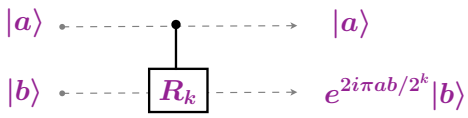
Portes utilisées

- Porte Hadamard

- Porte de décalage de phase



- Porte de déphasage controlée



Ecriture binaire

- Ecriture binaire de $x \in \mathbb{Z}_{2^n}$: $x = \sum_{i=1}^{n} x_i 2^{n-i}$ avec $x_i \in \{0,1\}$

$$x \in \mathbb{Z}_{2^n} \leftrightarrow (x_1, \ldots, x_n) \in (\mathbb{Z}_2)^n$$

Construction de la transformée de Fourier sur $\mathbb{Z}_{2^n}$

Transformée de Fourier en écriture binaire

- Exercice : Montrer par récurrence que

$$|x\rangle \mapsto \frac{1}{2^{n/2}}(|0\rangle + e^{(2i\pi)0.x_n}|1\rangle)(|0\rangle + e^{(2i\pi)0.x_{n-1}x_n}|1\rangle)\ldots(|0\rangle + e^{(2i\pi)0.x_1x_2\ldots x_n}|1\rangle)$$

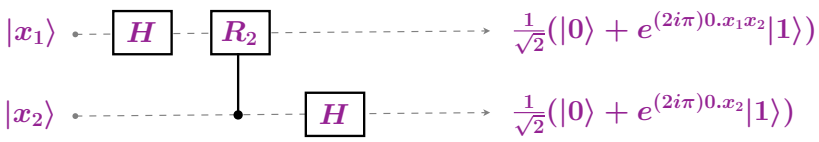
écriture binaire

Cas $n = 1$

- Transformée cyclique = Transformée de Hadamard

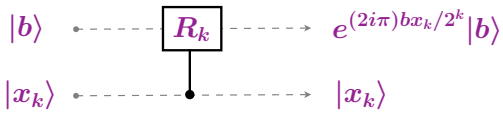
Cas $n = 2$

- Exercice : Monter que

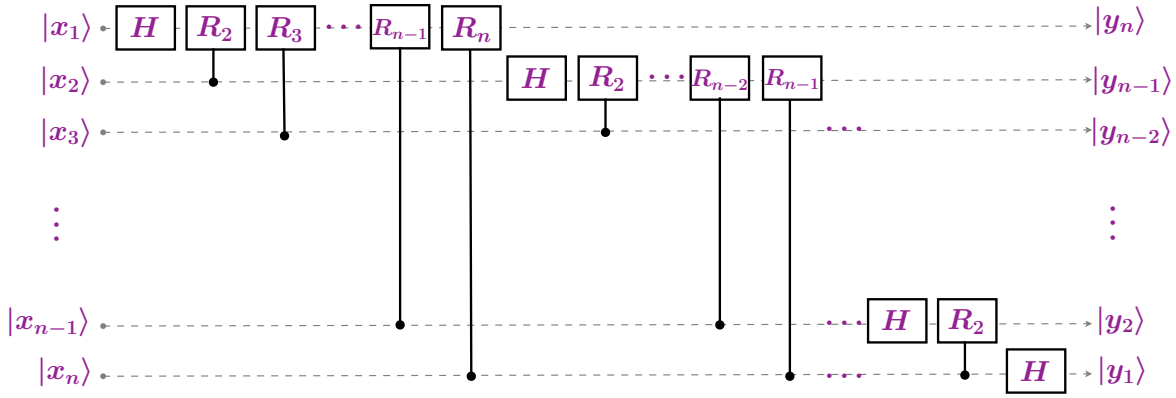


Circuit complet de la transformée de Fourier sur $\mathbb{Z}_{2^n}$

Rappel



Circuit complet



$$|y_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{(2\pi i)0.x_1x_2\ldots x_k}|1\rangle)$$

STOP Il faut inverser les qubits en sortie !

Généralisations

Théorème

- Il existe une famille uniforme de circuits de taille $(\log N)^2$ simulant exactement $QFT_{\mathbb{Z}_N}$ lorsque les facteurs premiers de N sont bornés

Théorème

- Il existe une famille uniforme de circuits de taille $(\log N)^3$ simulant exactement $QFT_{\mathbb{Z}_N}$ pour tout N

Théorème

- Il existe une famille uniforme de circuits de taille

$$O(\log N \log((\log N)/\varepsilon) + \log^2(1/\varepsilon))$$

simulant $QFT_{\mathbb{Z}_N}$ avec précision $\varepsilon > 0$

Généralisation

Problème du sous-groupe caché

- Entrée : G un groupe et f une fonction sur G telle que, pour un sous-groupe $H \leq G$ inconnu,
$$f(x) = f(y) \iff x^{-1}y \in H$$
- Sortie : un ensemble de générateurs de H

Exemples

- Problème de Simon : $G = (\mathbb{Z}_2)^n$, $H = \{0, s\}$
- Factorisation : $G = \mathbb{Z}$, $H = r\mathbb{Z}$
- Logarithme discret : $G = \mathbb{Z}^2$, $H = \{(rx, x) : x \in \mathbb{Z}\}$
- Equation de Pell : $G = \mathbb{R}$
- Isomorphisme de graphe : $G = \mathcal{S}_n$

Théorème : Algorithmes quantiques connus pour le pb du ss-groupe caché

- Groupe abélien de type fini : $\mathrm{poly}(\log|G|)$
- Groupe *doucement* résoluble : $\mathrm{poly}(\log|G|)$
- Groupe dihédral : $2^{O(\sqrt{\log|G|})}$
- Groupe quelconque : $\mathrm{poly}(\log|G|)$ requêtes, temps $2^{O(\log|G|)}$

Combien d'algorithmes quantiques existe-t-il ?

Problèmes sans structure

- Algorithme de Grover 1996

Problèmes avec une structure algébrique

- Algorithme de Shor 1994

Problèmes très structurés

- Les algorithmes classiques sont optimaux !

Problème un peu structurés

- Algorithme d'Ambainis 2003

  utilisation de marches quantiques (analogues des marches aléatoires) pour améliorer l'implémentation de l'opérateur de Grover
- Exemples

  Element Distinctness : Grover$^2 \to O(N^{3/4})$, Ambainis $\to O(N^{2/3})$ ← optimal

  Triangle free : Grover$^2 \to O(N^{3/2})$, Ambainis$^2 \to O(N^{1.3})$ ← *sans doute* non optimal...