Informatique Quantique

Frédéric Magniez

Cours 4 :
Algorithmes de Shor

Transformée de Fourier discrète

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

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

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

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

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

Portes utilisées

- Porte Hadamard

$$|b\rangle \dashrightarrow \boxed{H} \dashrightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

- Porte de décalage de phase

$$|b\rangle \dashrightarrow \boxed{R_k} \dashrightarrow e^{2i\pi b/2^k}|b\rangle$$

- Porte de déphasage controlée

$$|a\rangle \dashrightarrow |a\rangle$$
$$|b\rangle \dashrightarrow \boxed{R_k} \dashrightarrow e^{2i\pi ab/2^k}|b\rangle$$

Ecriture binaire

- Représentation : $x \in \mathbb{Z}_{2^n} \leftrightarrow (x_1, \ldots, x_n) \in (\mathbb{Z}_2)^n \qquad x_i \in \{0,1\}$

$$\frac{x}{2^n} = \sum_{i=1}^{n} x_i 2^{-i} = 0, x_1 x_2 \ldots x_n$$

- Simplification

$$\omega_N^{2^k x} = \omega_N^{0.x_{k+1}x_{k+2}\ldots x_n}$$

Transformée de Fourier en écriture binaire

- Exercice : Montrer que

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_N^{xy}|y\rangle = \frac{1}{2^{n/2}}(|0\rangle + \omega^{2^{n-1}x}|1\rangle)(|0\rangle + \omega^{2^{n-2}x}|1\rangle)\ldots(|0\rangle + \omega^{x}|1\rangle)$$
$$= \frac{1}{2^{n/2}}(|0\rangle + e^{(2i\pi)0.x_n}|1\rangle)(|0\rangle + e^{(2i\pi)0.x_{n-1}x_n}|1\rangle)\ldots(|0\rangle + e^{(2i\pi)0.x_1x_2\ldots x_n}|1\rangle)$$

écriture binaire

Transformée de Fourier inverse

- Etant donné $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_N^{xy}|y\rangle$ comment retrouver x ?

Cas n=1

- Trouver x_1 étant donné $\frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0.x_1}|1\rangle)$

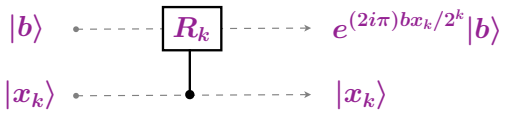
Cas n=2

- Trouver x_1 et x_2 étant donné

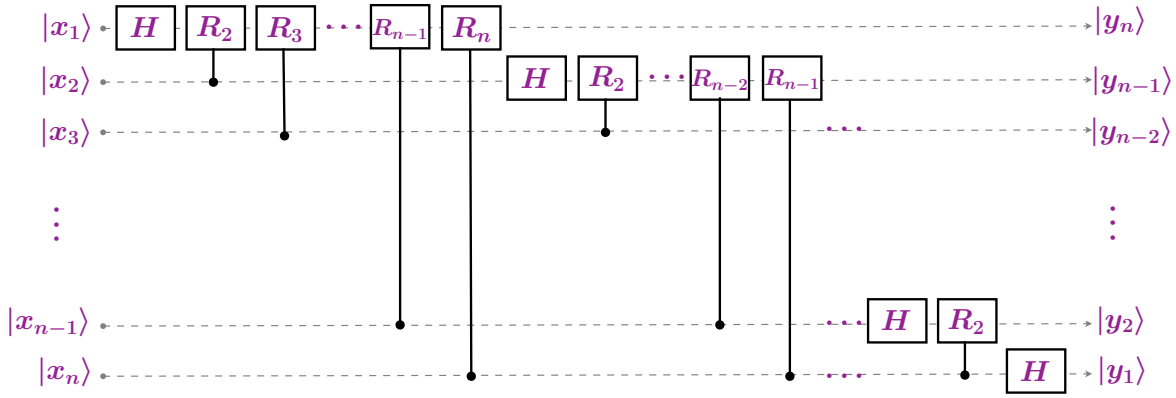
$$\frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0.x_2}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0.x_1x_2}|1\rangle)$$

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 $\varepsilon > 0$

Estimation de phase

Problème

- Entrée : un état $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{i\phi y}|y\rangle$ pour un angle $\phi \in [0, 2\pi[$
- Sortie : les n premiers bits de $\frac{\phi}{2\pi}$

Solution

- Cas $x = 2^n \frac{\phi}{2\pi}$: La transformée de Fourier inverse donne x
- Cas général : La transformée de Fourier inverse donne x telle que

$$\Pr\left(\left|\frac{x}{2^n} - \phi\right| \leq \frac{1}{2^n}\right) \geq \frac{8}{\pi^2} \approx 0,81$$

Application : Estimation de valeur propre

- Entrée
  - Des boîtes noires réalisant c-U^t pour U unitaire et t=1,2,...,2^n
  - Un état $|\Phi\rangle$ vecteur propre de U pour la valeur propre $e^{i\phi}$
- Sortie
  - La valeur de ϕ à n bits de précision près
- Exercice : montrer comment résoudre le problème avec la QFT inverse
  - Indication : construire l'état $\frac{1}{\sqrt{2^n}} \sum e^{i\phi y}|y\rangle$ avec n boîtes c-U^t

Utilisation : calcul de l'ordre

Problème

- Entrée : $N, a \in \mathbb{N}$ tels que $\text{pgcd}(a, N) = 1$
- Sortie : le plus petit entier $r \neq 0$ tel que $a^r = 1 \mod N$

Encodage

- Groupe des inversibles : $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N : \text{pgcd}(x, N) = 1\}$
- Fonction puissance : $f_a : \mathbb{Z} \to \mathbb{Z}_N^*,\ x \mapsto a^x$

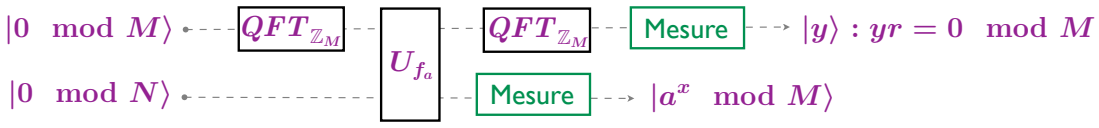
Propriétés

- f_a est périodique de période r
- Si $f_a(x) = f_a(y)$ alors $r|(x - y)$

Obstacle

- On souhaiterait un multiple M de r pour utiliser l'algorithme de recherche de période dans $\mathbb{Z}_M$ à l'aide de $QFT_{\mathbb{Z}_M}$
- Mais trouver un tel $M = \text{poly}(N)$ est *à peu près* aussi difficile que factoriser N

Cas facile : $r|M$



Initialisation : $|0 \mod M\rangle|0 \mod N\rangle$

Parallélisation : $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|0\rangle$

Appel de f_a: $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|a^x \mod N\rangle \qquad 0 \leq x < r$

Mesure partielle : $\sqrt{\frac{r}{M}} \sum_{j=0}^{M/r-1} |x + jr\rangle|a^x \mod N\rangle$

Interférences : $\frac{\sqrt{r}}{M} \sum_{y=0}^{M-1} \omega_M^{xy} \Big(\sum_{j=0}^{M/r-1} (\omega_M^{ry})^j \Big) |y\rangle|a^x \mod N\rangle$

$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{xk} |kM/r\rangle|a^x \mod N\rangle$

STOP $y \cdot s = 0 \leftrightarrow yr = 0 \mod M : y = kM/r,\ k = 0, \ldots, r-1$

Retrouver r

Bilan

- Avec probabilité uniforme sur $k = 0, \ldots, r-1$ on observe $y = kM/r$
- La décomposition en fraction irréductible de y/M renvoie t/z telle que $z|r$

Théorème

$$\Pr_{k,k'=0,\ldots,r-1}[\text{ppcm}(z, z') = r] \geq 0.4$$

Conclusion

- Si $r|M$, alors avec deux exécutions de l'algorithme de Shor, on obtient un facteur non trivial de N avec probabilité $\Omega(1)$

Remarque

- On peut vérifier qu'on a trouver le bon ordre car

$$(r'|r \text{ et } a^{r'} = 1) \implies r' = r$$

Cas difficile : $r \not| M$

Choix de M

- Contrainte : $N^2 < M < 2N^2$
- Pour simplifier la transformée de Fourier : $M = 2^m$

Même algorithme...

- Même sommation globale — en fait $\lfloor M/r \rfloor$ ou $\lfloor M/r \rfloor + 1$

$$\frac{\sqrt{r}}{M} \sum_{y=0}^{M-1} \omega_M^{xy} \Big(\sum_{j=0}^{M/r-1} (\omega_M^{ry})^j \Big) |y\rangle |a^x \mod N\rangle$$

- Après mesure

  Précédemment

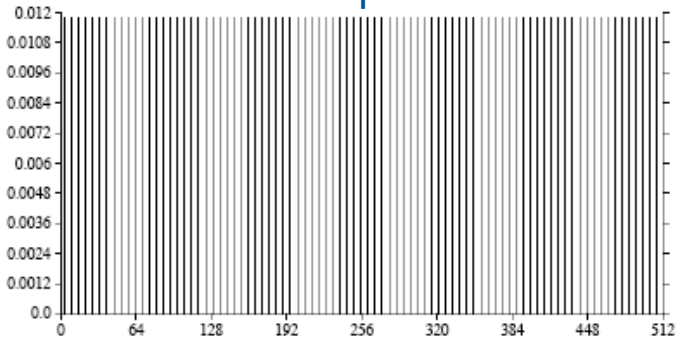
  $$\Pr_y[yr = 0 \mod M] = 1$$

  Maintenant

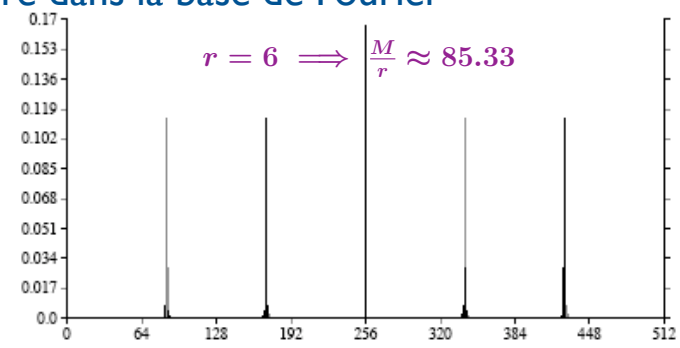
  $$\Pr_y[|yr|_{\mod M} \leq r/2] \geq \frac{1}{3r^2}$$

Exemple : $N = 21, a = 11, M = 2^9$

Mesure dans la base classique



Mesure dans la base de Fourier



Retrouver q (bis)

Préliminaires

- Supposons : $|yr|_{\mathrm{mod}\, M} \leq r/2$
- Alors il existe un entier $k \geq 0$ tel que

$$-\frac{r}{2} \leq yr - kM \leq \frac{r}{2}$$
$$-\frac{1}{2M} \leq \frac{y}{M} - \frac{k}{r} \leq \frac{1}{2M}$$

- L'hypothèse $M > N^2$ assure l'unicité de la fraction $\frac{k}{r}$ effectuant une telle approximation avec un dénominateur $\leq N$

Théorème : Fractions continues

- Trouver la meilleur approximation d'une fraction par une fraction de dénominateur $\leq N$ s'effectue en temps $O(\log^3 N)$

  http://serge.mehl.free.fr/anx/fraction_cont.html

Conclusion

- Avec probabilité $\geq \frac{1}{3r^2}$ on génère une fraction $\frac{k}{r}$ avec k aléatoire
- Reste à appliquer la méthode du cas simple sur toutes les paires d'un échantillon de taille $O(\log r)$
- Alors le plus petit des candidats r' tq $a^{r'} = 1 \mod N$ est bien r avec *grande* probabilité

Exercice : Factoriser avec l'estimation de valeur propre

Opérateur Multiplication

- Soit a un entier modulo N, premier avec N, d'ordre r
- Soit la transformation : $U_a : |x\rangle \mapsto |ax\rangle$
- Montrer que : $(U_a)^t = U_{a^t}$
- En déduire que les valeurs propres λ de U_a satisfont $\lambda^r=1$
- Montrer que chaque vecteur $|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \omega_r^{jk} |a^j\rangle$ est vecteur propre de U_a pour une valeur propre à calculer

Factoriser

- Montrer qu'en partant d'une superposition uniforme de vecteurs propres $|\psi_k\rangle$ de U_a, alors l'estimation de valeur propre fourni un y tq $y/N=k/r$
- Quelle est la superposition uniforme des vecteurs propres $|\psi_k\rangle$ de U_a
- Conclure avec un autre algorithme pour la factorisation. Donner sa taille.

Lemme

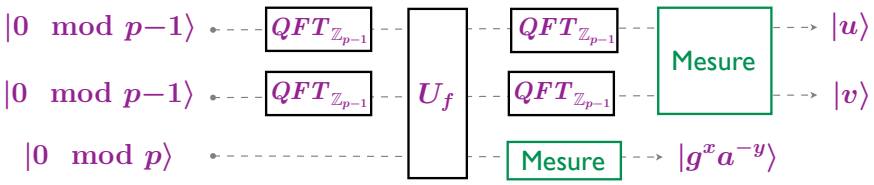
- Si p est premier alors $\mathbb{Z}_p^*$ est cyclique de taille $p-1$

Problème

- Entrées
  - Un entier p premier et un générateur g de $\mathbb{Z}_p^*$:
    $\mathbb{Z}_p^* = \{g^x \mod p : x = 0, 1, \ldots, p-2\}$
  - Un élément $a \in \mathbb{Z}_p^*$
- Sortie : l'entier $r \in \{0, \ldots, p-2\}$ tel que $a = g^r \mod p$

Application

- Algorithme de Diffie-Hellman :
  - Alternative à RSA sur une courbe elliptique
  - clé de 160 bits ≈ factoriser 1024 bits



- Justifier qu'on peut supposer avoir un circuit réalisant exactement $QFT_{\mathbb{Z}_{p-1}}$
- On pose $f(x,y) = g^x a^{-y}$
- Montrer que f satisfait
  $f(x,y) = f(x',y') \iff \exists k,\ (x',y') = (x,y) + k(r,1)$
- Calculer l'état du système après la première mesure partielle
- Calculer l'état du système avant la dernière mesure
- Montrer que
  $\Pr_{u,v}[ur + v = 0 \mod p-1] = 1$
- Conclure

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

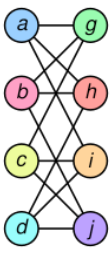
- Problème de Simon : $G = (\mathbb{Z}_2)^n$, $H = \{0, s\}$
- Factorisation : $G = \mathbb{Z}$, $H = r\mathbb{Z}$
- Logarithme discret : $G = \mathbb{Z}^2$, $H = \{(rx, x) : x \in \mathbb{Z}\}$
- Equation de Pell : $G = \mathbb{R}$
- Isomorphisme de graphe : $G = \mathcal{S}_n$

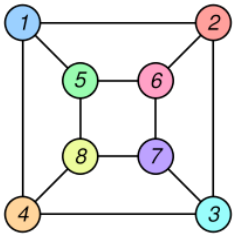
Théorème : Algorithmes quantiques connus pour le pb du ss-groupe caché

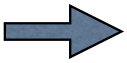
- Groupe abélien de type fini : $\mathrm{poly}(\log|G|)$
- Groupe *doucement* résoluble : $\mathrm{poly}(\log|G|)$
- Groupe dihédral : $2^{O(\sqrt{\log|G|})}$
- Groupe quelconque : $\mathrm{poly}(\log|G|)$ requêtes, temps $2^{O(\log|G|)}$

Problème

- Entrée : 2 graphes *G* et *H* sur *n* sommets
- Sortie : Une bijection *f* qui envoie les sommets de *G* sur ceux de *H*, telle que les 2 graphes coïncident
- Application : chimie moléculaire, conception de circuits







G	H
a	1
b	6
c	8
d	3
e	5
f	2
g	4
h	7

Réduction au pb du sous-groupe caché

- Groupe : ensemble $\mathcal{S}_{2n}$ des bijections sur les sommets de *G* et *H*
- Fonction : $\pi \in \mathcal{S}_{2n} \mapsto \pi(G \cup H)$
- Sous-groupe caché (cas des graphes rigides) :
  $\{\mathrm{Id}\}$ si non-isomorphes
  $\{\mathrm{Id}, \pi\}$: $\pi(G) = H$, $\pi(H) = G$ sinon

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$^2 \rightarrow O(N^{3/4})$, Ambainis $\rightarrow O(N^{2/3})$ ← optimal

  Triangle free : Grover$^2 \rightarrow O(N^{3/2})$, Ambainis$^2 \rightarrow O(N^{1.3})$

  ← *sans doute* non optimal...