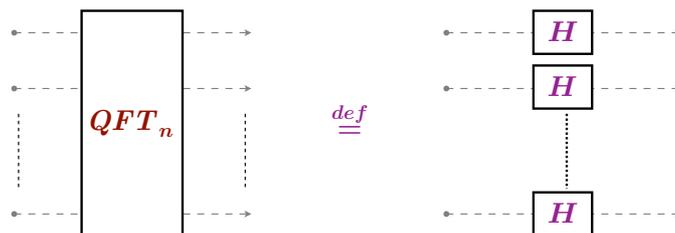


# Informatique Quantique

Frédéric Magniez

## Cours 4 : Transformée de Fourier quantique Algorithmes de Shor

### Rappels



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

$$\text{avec } x \cdot y = \sum_i x_i y_i \pmod{2}$$

## Transformée de Fourier discrète

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

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

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

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

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

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

## 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

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

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

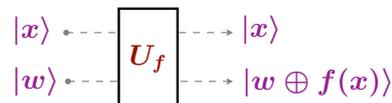
## Le problème de Simon

### Problème

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

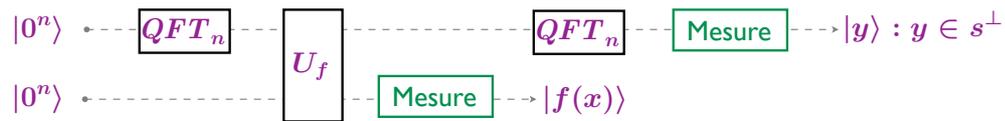


### Complexité en requêtes

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

### Idée

Utiliser  $QFT$  pour rechercher la période  $s$ .



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 :  $y_1, y_2, \dots, y_{n+k} \in s^\perp$
- 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

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

### Preuve

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

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

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

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

## Exercices

### 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  $f, g : \{0, 1\}^n \rightarrow \{0, 1\}^n$  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  $\text{poly}(\log|G|)$
- **Calcul de l'ordre** se résout en temps quantique polynomial  
Entrée :  $N, a \in \mathbb{N}$  tels que  $\text{pgcd}(a, N) = 1$   
Sortie : le plus petit entier  $r \neq 0$  tel que  $a^r = 1 \pmod{N}$

## Factorisation

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

**Réduction** : Factorisation  $\leq_R$  Calcul de l'ordre

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

## Transformée de Fourier sur le groupe cyclique

### Transformée de Fourier discrète

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

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

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

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

### Analogie 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

$$\begin{aligned} QFT_{\mathbb{Z}_N} : |x\rangle &\mapsto \frac{1}{\sqrt{N}} \sum_y \omega_N^{xy} |y\rangle \\ |f\rangle = \sum_x f(x) |x\rangle &\mapsto \frac{1}{\sqrt{N}} \sum_y \overline{\hat{f}(y)} |y\rangle \end{aligned}$$

car on n'a pas conjugué  $\omega$  par commodité

### Portes utilisées

- Porte Hadamard

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

- Porte de décalage de phase

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

- Porte de déphasage contrôlée

$$\begin{array}{ccc} |a\rangle & \xrightarrow{\bullet} & |a\rangle \\ & \downarrow & \\ |b\rangle & \xrightarrow{R_k} & e^{2i\pi ab/2^k}|b\rangle \end{array}$$

### Écriture binaire

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

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

- Simplification

$$\omega_N^{2^k x} = \omega_N^{0, x_{k+1} x_{k+2} \dots x_n}$$

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

### Transformée de Fourier en écriture binaire

- Exercice : Montrer que

$$\begin{aligned} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_N^{xy} |y\rangle &= \frac{1}{2^{n/2}} (|0\rangle + \omega^{2^{n-1}x} |1\rangle) (|0\rangle + \omega^{2^{n-2}x} |1\rangle) \dots (|0\rangle + \omega^x |1\rangle) \\ &= \frac{1}{2^{n/2}} (|0\rangle + e^{(2i\pi)0, x_n} |1\rangle) (|0\rangle + e^{(2i\pi)0, x_{n-1} x_n} |1\rangle) \dots (|0\rangle + e^{(2i\pi)0, x_1 x_2 \dots x_n} |1\rangle) \end{aligned}$$

écriture binaire

### Cas $n=1$

- Exercice : Etant donné  $x_1$ , donner le circuit qui produit

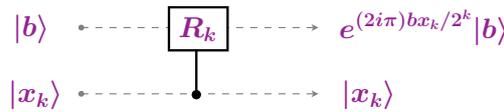
$$\frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0, x_1} |1\rangle)$$

### Cas $n=2$

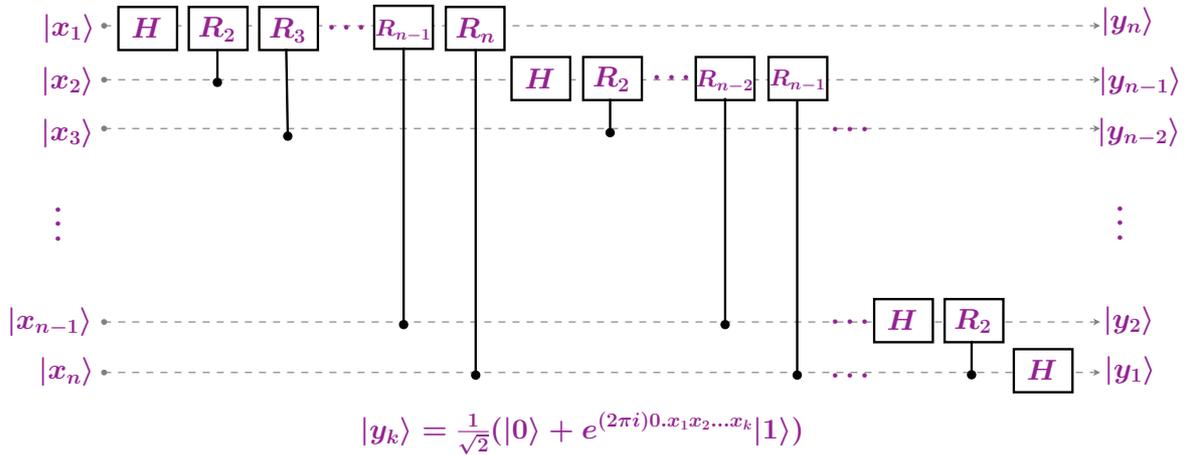
- Exercice : Etant donnés  $x_1$  et  $x_2$ , donner le circuit qui produit

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0, x_2} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{(2i\pi)0, x_1 x_2} |1\rangle)$$

Rappel



Circuit complet



**STOP** Il faut inverser les qubits en sortie !

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  $O(\log N \log((\log N)/\epsilon) + \log^2(1/\epsilon))$  simulant  $QFT_{\mathbb{Z}_N}$  avec précision  $\epsilon > 0$

### Problème

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

### Encodage

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

### 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  $QFT_{\mathbb{Z}_M}$
- Solution : prendre  $M$  suffisamment grand pour que  $M$  soit à peu près un multiple de  $r$

Dans la suite on suppose que  $M$  est un multiple de  $r$

### Cas facile : $r | M$



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

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

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

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

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

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



$y \cdot s = 0 \leftrightarrow yr = 0 \pmod M : y = kM/r, k = 0, \dots, r - 1$

## Bilan

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

## Théorème

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

## 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 trouvé le bon ordre car
 
$$(r'|r \text{ et } a^{r'} = 1) \implies r' = r$$

## Lemme

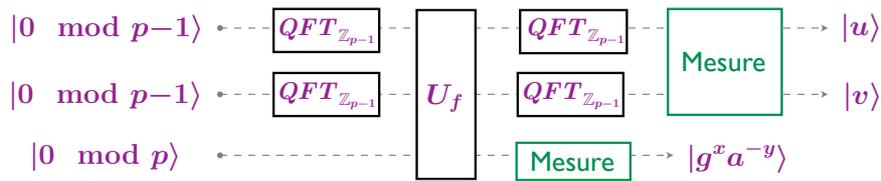
- Si  $p$  est premier alors  $\mathbb{Z}_p^*$  est cyclique de taille  $p - 1$

## Problème

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

## Application

- **Algorithme de Diffie-Hellman** :
  - Alternative à RSA sur une courbe elliptique
  - clé de 160 bits  $\approx$  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
 
$$\Pr_{u,v}[ur + v = 0 \pmod{p-1}] = 1$$
- 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

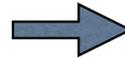
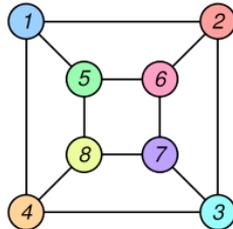
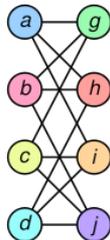
- Problème de Simon :  $G = (\mathbb{Z}_2)^n, H = \{0, s\}$
- Factorisation :  $G = \mathbb{Z}, H = r\mathbb{Z}$
- Logarithme discret :  $G = \mathbb{Z}^2, H = \{(rx, x) : x \in \mathbb{Z}\}$
- Equation de Pell :  $G = \mathbb{R}$
- Isomorphisme de graphe :  $G = \mathcal{S}_n$

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

- Groupe abélien de type fini :  $\text{poly}(\log|G|)$
- Groupe quelconque :  $\text{poly}(\log|G|)$  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) :
  - $\{\text{Id}\}$  si non-isomorphes
  - $\{\text{Id}, \pi\}$  :  $\pi(G) = H, \pi(H) = G$  sinon

### 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<sup>2</sup>  $\rightarrow O(N^{3/4})$ , Ambainis  $\rightarrow O(N^{2/3})$

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

← optimal  
← sans doute non optimal...