INF581: Information Quantique **Hiver 2010**

Cours 7 — 1 mars

Enseignant : Philippe Grangier – Frédéric Magniez Rédacteur : de Portzamparc-Miglietti

7.1 Le problème général du sous groupe caché

7.1.1 Enoncé

Soit G un groupe et f une fonction agissant sur G telle qu'il existe $H \subseteq G$ tel que

$$f(x) = f(y) \Longleftrightarrow x^{-1}y \in H$$

Comment trouver un ensemble de générateurs de H ?

7.1.2 Résultats

La résolution par des algorithmes quantiques du problème du sous groupe caché dépend de la structure de G.

- Pour G groupe abélien de type fini temps $poly(log|G|)$
- Pour G groupe quelconque : $poly(log|G|)$ requetes , temps de calcul $2^{O(log|G|)}$

7.2 Des exemples au problème du sous groupe caché

7.2.1 Le problème de Simon $G = (Z_2)^n$ et $H = \{0, s\}$

Enoncé

Soit $f : \{0,1\}^n \to \{0,1\}^n$ telle que

$$\exists s \in \{0,1\}^n : \forall x \neq y,\ f(x) = f(y) \Longleftrightarrow x = y \oplus s$$

f est une boite noire et le but est donc de trouver s.

Solution quantique

On utilise la tranformée de Fourier quantique QFT de manière suivante :
Suivons l'evolution des 2 qubits au cours du montage :

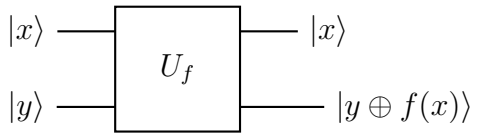

FIGURE 7.1. Boite noire de f

Initialisation	$\|0^n > \|0^n >$
Parallélisation	$\frac{1}{2^{\frac{n}{2}}} \sum \|x > \|0^n >$
Appel de f	$\frac{1}{2^{\frac{n}{2}}} \sum \|x > \|f(x) >$
Mesure partielle	$\frac{1}{\sqrt{2}}(\|x > + \|x \oplus s >)\|f(x) >$
Interférences	$\frac{1}{2^{\frac{n+1}{2}}} \sum_y \left((-1)^{x.y} + (-1)^{(x \oplus s).y}\right) \|y > \|f(x) >$
	$\frac{1}{2^{\frac{n+1}{2}}} \sum_y (-1)^{x.y} \left(1 + (-1)^{s.y}\right) \|y > \|f(x) >$
	$\frac{1}{2^{\frac{n-1}{2}}} \sum_{y : s \cdot y = 0} (-1)^{x.y} \|y > \|f(x) >$

On notera l'intéret de la mesure partielle qui sert à projeter les y tels que $f(y) = f(x)$.

Système

En sortie on obtient une série de vecteur y orthogonaux à s. Après $n + k$ itérations on obtient $n + k$ vecteurs orthogonaux à s. D'après des résultats sur les groupes finis les $n + k$ vecteurs forment une famillle de rang n avec probabilité $p \geq 1 - \frac{1}{2^k}$ si $s = 0^n$ et $q \geq 1 - \frac{1}{2^{k+1}}$ sinon. Dans ce cas le systeme

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

admet en plus de la solution triviale nulle le vecteur s. La complexité en requete est donc $O(n)$ et La résolution d'un tel système se fait en temps $O(n^3)$.

Justification du rang du système

Rappelons qu'on est ici dans le cadre d'un groupe de la forme $\mathbb{Z}_2^n$. Il est utile de le considérer non seulement comme un groupe, mais aussi comme un $\mathbb{Z}_2$-espace vectoriel.

Alors pour H un hyperplan de G et x un élément tiré au hasard dans G, H étant un sous-espace de dimension $n - 1$, card $H = 2^{n-1}$ et $\Pr(x \in H) = 1/2$.

Alors, pour $x_1, \ldots, x_l$ choisis au hasard dans G.

$$\begin{aligned}\Pr(< x_1, \ldots, x_l > \subseteq H) &= \Pr(x_1 \in H, \ldots, x_l \in H) \\ &= \Pr(x_1 \in H) \ldots \Pr(x_l \in H) \\ &= \tfrac{1}{2^l}\end{aligned}$$

On s'intéresse à la probabilité contraire : dire que les vecteurs $y_1, y_2, \ldots y_{n+k}$ n'engendrent pas tout l'espace, c'est dire qu'il existe un hyperplan qui les contient tous. Comme il y a autant d'hyperplans que de vecteurs non-nuls (ce sont leurs orthogonaux), on peut écrire :

$$\begin{aligned}\Pr(\exists H \text{ hyperplan } / < y_1, y_2, \ldots y_{n+k} > \subseteq H) &= \Pr\left(\bigcup_{H \text{ hyperplan}} < y_1, y_2, \ldots y_{n+k} > \subseteq H\right) \\ &\leq \sum_{H \text{ hyperplan}} \Pr(< y_1, y_2, \ldots y_{n+k} > \subseteq H) \\ &\leq \tfrac{2^n - 1}{2^{n+k}} \\ &\leq \tfrac{1}{2^k}\end{aligned}$$

Donc les $y_1, y_2, \ldots y_{n+k}$ sont générateurs avec probabilité $p \geq 1 - \frac{1}{2^k}$.

7.2.2 Application de l'algorithme de Simon au cas $G = (\{0,1\}^n, \oplus)$ et H quelconque

Enoncé

Soit $f : \{0,1\}^n \to \{0,1\}^n$ telle que

$$\forall x \neq y,\ f(x) = f(y) \Longleftrightarrow x - y \in H$$

Application de l'algorithme de Simon

Initialisation	$\lvert 0^n > \lvert 0^n >$
Parallélisation	$\frac{1}{2^{\frac{n}{2}}} \sum \lvert x > \lvert 0^n >$
Appel de f	$\frac{1}{2^{\frac{n}{2}}} \sum \lvert x > \lvert f(x) >$
Mesure partielle	$\frac{1}{\sqrt{\lvert H \rvert}} \left(\sum_{h \in H} \lvert x \oplus h > \right) \lvert f(x) >$
Interférences	$\frac{1}{\sqrt{\lvert H \rvert} 2^{\frac{n}{2}}} \sum_y \left(\sum_{h \in H} (-1)^{y \cdot (x \oplus h)} \right) \lvert y > \lvert f(x) >$
	$\frac{1}{\sqrt{\lvert H \rvert} 2^{\frac{n}{2}}} \sum_y (-1)^{x \cdot y} \sum_{h \in H} (-1)^{y \cdot h} \lvert y > \lvert f(x) >$

Or si $y \in H^\perp \sum_{h \in H} (-1)^{y \cdot h} = |H|$.

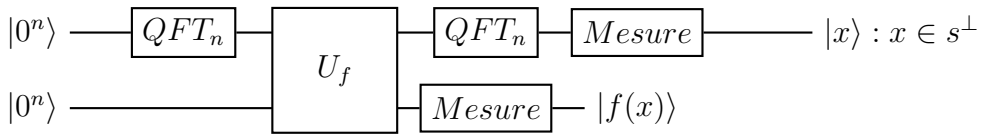

Figure 7.2. Schéma quantique pour l'algorithme de Simon

Sinon en posant $H_0 = \{h \in H : y \cdot h = 0\}$ et $H_1 = \{h \in H : y \cdot h = 1\}$, on a H_1 non vide : il contient au moins un élément h_1. En notant g l'application

$$\begin{array}{ccc} H_0 & \to & H_1 \\ h & \to & h \oplus h_1 \end{array}$$

et g'

$$\begin{array}{ccc} H_1 & \to & H_0 \\ h & \to & h \oplus h_1 \end{array}$$

on a $g \circ g' = g' \circ g = id$ et donc H_0 et H_1 sont en bijection et sont donc de meme cardinal : $|H_1| = |H_0|$.

On obtient $\sum_{h \in H} (-1)^{y \cdot h} = 0$ si $y \notin H^\perp$.

Au final on a l'état

$$\frac{\sqrt{|H|}}{2^{\frac{n}{2}}} \sum_{y \in H^\perp} (-1)^{x \cdot y} |y> |f(x)>$$

Ce qui nous donne des vecteurs orthogonaux à H. Au bout de $|G| - |H| + k$ itérations on obtient $|G| - |H| + k$ vecteurs orthogonaux qui forment une famille de rang $|G| - |H|$ avec probabilité $q \geq 1 - \frac{1}{2^{k+1}}$. On peut ainsi construire un sytème dont la résolution donne $|H|$ générateurs indépendants de H et donc une famillle génératrice de H.

7.2.3 Calcul de l'ordre d'un élément modulo N et Factorisation $G = \mathbb{Z}$ et $H = r\mathbb{Z}$

Enoncé du calcul de l'ordre

Etant donnés N et $a \in \mathbb{N}$ tels que $pgcd(a, N) = 1$, trouver le plus petit entier $r \neq 0$ tel que $a^r = 1 \ mod \ N$. On se ramène au problème du sous-groupe caché en considérant la fonction :

$$f_a : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & (\mathbb{Z}_N)^* \\ x & \longmapsto & a^x \end{array}$$

f_a est bien une fonction du type considéré : f_a est périodique de période r par définition de l'ordre. De plus si $f_a(x) = f_a(y)$ alors $r \mid (x - y)$, c'est à dire $x - y \in r\mathbb{Z}$. Le sous-groupe caché est donc ici $H = r\mathbb{Z}$. Pour poursuivre la présentation de l'algorithme, on a besoin de la transformée de Fourier sur un groupe cyclique.

Transformée de Fourier $QFT_{\mathbb{Z}_N}$ sur le groupe cyclique

On prend comme base de Fourier de l'espace des fonctions $f : \mathbb{Z}_N \to \mathbb{C}$ la famille $(\chi_y)_{y\in\mathbb{Z}_N}$ telle que $\chi_y(x) = \omega_N^{xy} = e^{2i\pi xy/N}$.

A un vecteur $|x>$ on associe $\frac{1}{\sqrt{N}}\sum_y \omega_N^{xy}|y>$.

On réalise ceci grace à une famille uniforme de circuits simulant exactement $QFT_{\mathbb{Z}_N}$ de taille $(logN)^2$ lorsque les facteurs premiers de N sont bornés et $(logN)^3$ sinon.

Retour sur le calcul de l'ordre

Soit $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N : pgcd(x, N) = 1\}$ et $f_a : \mathbb{Z} \to \mathbb{Z}_N^*, x \to a^x$. f_a est périodique de période r et $f_a(x) = f_a(y)$ alors $r|(x - y)$.

- Si on connaissait un multiple M de r on pourrait utiliser l'algorithme de Simon de recherche de période dans $\mathbb{Z}_M$ à l'aide de $QFT_{\mathbb{Z}_M}$. On obtient alors le schéma quantique suivant :

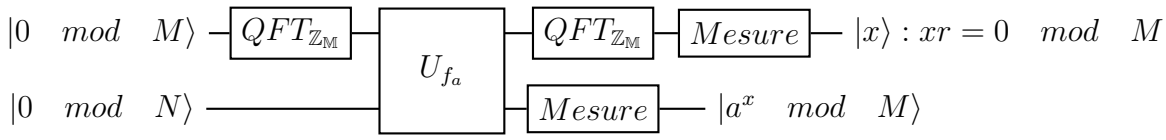

Figure 7.3. Schéma quantique pour le calcul de l'ordre

Initialisation	$\|0 \bmod M> \|0 \bmod N>$
Parallélisation	$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \|x> \|0>$
Appel de f_a	$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \|x> \|a^x \bmod N>$
Mesure partielle	$\sqrt{\frac{r}{M}} \sum_{j=0}^{M/r-1} \|x + jr> \|a^x \bmod N>$
Interférences	$\frac{\sqrt{r}}{M} \sum_{y=0}^{M/r-1} \omega_M^{xy} \left(\sum_{j=0}^{M/r-1} (\omega_M^{ry})^j \right) \|y> \|a^x \bmod N>$
Seuls restent les $y/ry \equiv 0(M)$	$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{xk} \|kM/r> \|a^x \bmod N>$ en posant $y = \frac{kM}{r}$

On observe donc ainsi des multiples du rapport $\frac{M}{r}$. En l'éxecutant deux fois on obtient $\frac{k_1 M}{r}$ et $\frac{k_2 M}{r}$.

On calcule alors $\gcd(\frac{k_1 M}{r}, \frac{k_2 M}{r}) = \frac{M}{r} \gcd(k_1, k_2)$. Or on peut donc démontrer que $\Pr(\gcd(k_1, k_2) = 1) \geq 0,4$. Ceci permet donc de trouver r avec une probabilité supérieure à $0,4$.

On peut vérifier qu'il s'agit bien de la période car dans les mauvais cas on trouve des diviseurs de r, donc des r' qui ne vérifient pas $a^{r'} \equiv 1 \bmod N$.

- Sinon on choisit M tel que $M = 2^m$ et $N^2 < M < 2N^2$. On apllique le meme algorithme. La ou on avait $\underset{y}{Pr}[yr = 0 \, mod \, M] = 1$ on a maintenant $\underset{y}{Pr}[|yr|_{mod\, M} \leq r/2] \geq \frac{1}{3}$. Dès lors si $|yr|_{mod\, M} \leq r/2$ alors il existe un unique k tel que $yr = kM + |yr|_{mod\, M}$ et donc une unique fraction $\frac{k}{r}$ telle que $-\frac{1}{2M} \leq \frac{y}{M} - \frac{k}{r} \leq \frac{1}{2M}$. Cette unique fraction est trouvée par l'algorithme des fonctions continues en temps $O(log^3 N)$.
  On reitère le processus jusqu'a avoir un échantillon conséquent de fraction $\frac{k'}{r}$. En calculant le *ppcm* de toutes les paires de l'échantillon on obtient avec une grande probabilité le r recherché.

Application au calcul du logarithme discret

On se place sur $(\mathbb{Z}/p\mathbb{Z})^*$. Il s'agit d'un groupe cyclique. On peut utiliser la transformée de Fourier qu'on vient de définir pour calculer le logarithme discret d'un élément. On s'en donne g un générateur. On a alors

$$(\mathbb{Z}/p\mathbb{Z})^* = \{g^x\}_{x \in \mathbb{Z}/(p-1)\mathbb{Z}}$$

Le problème du logarithme discret consiste, étant donné un élément a de $(\mathbb{Z}/p\mathbb{Z})^*$, à trouver un $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ tel que $a = g^x$

On définit

$$f(x, y) = g^x a^{-y} = g^x \left(g^r\right)^{-y} = g^{x-ry}$$

Par définition de g, $f(x, y) = 1 \iff x - ry = 0$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Donc, en introduisant un paramètre k,

$$\begin{array}{rcl} f(x, y) = f(x', y') & \iff & \exists k / (x', y') = (x, y) + k(r, 1) \\ & \iff & (x', y') - (x, y) \in < (r, 1) > \text{ dans } \mathbb{Z}/(p-1)\mathbb{Z} \end{array}$$

On est donc ramené au problème du sous-groupe caché pour $G = \mathbb{Z}/(p-1)\mathbb{Z}$
On réalise le schéma suivant la méthode de Simon :
Après la première mesure, le système est dans l'état

$$\sum_k \mid x + kr > \mid y + k > \mid f(x, y) >$$

Avant la mesure finale, on obtient l'état

$$\sum_k \left(\sum_u \omega_{p-1}^{(x+kr)u} \mid u > \sum_v \omega_{p-1}^{(y+k)v} \mid v > \right) \mid f(x, y) > = \sum_{u,v} \omega_{p-1}^{xu+yv} \left(\sum_k \omega_{p-1}^{(ur+v)k} \right) \mid u, v > \mid f(x, y) >$$

On observe que si $ur + v \not\equiv 0 \bmod p - 1$, $\sum\limits_k \omega_{p-1}^{(ur+v)k} = 0$.

Donc on ne peut observer en sortie que des $\mid u, v >$ tels que

$$ur + v \equiv 0 \bmod p-1 \text{ i.e. } (u,v) \in <(r,1)>^{\perp}$$

Il s'agit bien de la même condition que dans le problème de Simon dans le cadre du groupe cyclique. On peut poursuivre l'analogie avec l'algorithme de Simon dans le cas $G = (\{0,1\}^n, \oplus$ en montrant d'une façon analogue (et en fait plus générale) que l'on ne peut mesurer que des vecteurs dans l'orthogonal du sous-groupe des périodes : H est ici un sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ et, si $y \notin H^{\perp}$, il existe $h_0 \in H / yh_0 \neq 0$ i.e. $yh_0 \not\equiv 0 \bmod p-1$, donc on a

$$\sum_{h\in H} \omega_{p-1}^{hy} \underset{[h=h_0+h']}{=} \sum_{h'\in H} \omega_{p-1}^{(h_0+h')y} = \omega_{p-1}^{h_0 y} \sum_{h\in H} \omega_{p-1}^{hy}$$

$$(1-\omega_{p-1}^{h_0 y}) \sum_{h\in H} \omega_{p-1}^{hy} = 0$$

Donc comme $yh_0 \not\equiv 0 \bmod p-1$, $\omega_{p-1}^{h_0 y} \neq 1$ et nécessairement $\sum_{h\in H} \omega_{p-1}^{hy} = 0$.

On peut alors calculer r dès que u est inversible dans $\mathbb{Z}/(p-1)\mathbb{Z}$, c'est à dire quand u et $p-1$ sont premiers entre eux. En tirant u au hasard, on a donc une probabilité $\frac{\phi(p-1)}{p-1}$ d'obtenir un nombre inversible. Elle dépend de la complexité arithmétique de $p-1$ du fait de l'expression de ϕ : si on a pour décomposition en facteurs premiers de $p-1$: $p-1 = q_1^{\alpha_1} \dots q_n^{\alpha_n}$, alors

$$\frac{\phi(p-1)}{p-1} = (1-\frac{1}{q_1}) \dots (1-\frac{1}{q_n})$$