Théorie des nombres algorithmique

2024-2025

Table des matières

Chapitre 1

Algorithmes

1.1 $\frac{3}{5}|0> +\frac{4}{5}|1>$

C'est un exo à la con mais c'est instructif, on regarde

$$\begin{aligned}|0> &\to \frac{1}{\sqrt{2}}(|0> +|1>)\\ &\to \frac{1}{\sqrt{2}}(|0> +e^{i\theta}|1>)\\ &\to \frac{1}{2}(|0> (1+e^{i\theta}) + |1> (1-e^{i\theta}))\\ &\to \frac{1}{2}(e^{i\theta/2}(e^{-i\theta/2}+e^{i\theta/2}) + e^{i\theta/2}|1> (e^{-i\theta/2}-e^{i\theta/2}))\end{aligned}$$

et là suffit d'ajuster theta puis de refaire des phases shifts.

1.2 Deutsch-Josza

Donc l'algorithme permet de décider si $f\colon 2^n \to 2$ est constante ou équilibrée (Comme un morphisme de groupes $(\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{F}_2$).

En gros le point crucial c'est que sur $|0^n > |1 >$ Si on fait $H^{\otimes(n+1)}$, U_f

puis $H^{\otimes n}$ on obtient :

$$\begin{aligned}|0^n>|1> &\to \sum_{x\in 2^n}|x>(|0>-|1>)\\ &\to \sum_{x\in 2^n}|x>(|f(x)>-|1\oplus f(x)>\\ &\to \sum_{y\in 2^n}|y>\sum_{x\in 2^n}(-1)^{f(x)}(-1)^{x.y}\end{aligned}$$

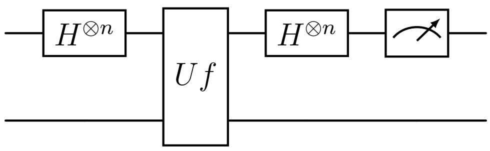
En particulier $||q_{0^n}|| = \sum_{x\in 2^n}(-1)^{f(x)}/2^n$. D'où si f est constant on obtient 0^n avec proba 1, sinon proba 0 d'avoir 0^n.

1.3 Simon

Cette fois c'est plus fun, si on prends

$$f\colon (\mathbb{Z}/2\mathbb{Z})^n \to X$$

avec X un ensemble fini, et si f vérifie $f(x) = f(y)$ ssi $x = y$ ou $x = y + a$ on aimerait trouver a. Essentielemment, si f passe au quotient en $< a >$ on veut trouver le "noyau". On regarde



À nouveau on fait rentrer $|0^{n+m}>$, on obtient

$$\begin{aligned}|0^{n+m}> &\to \frac{1}{2^{n/2}}\sum_{x\in 2^n}|x>|f(x)>\\ &\to \frac{1}{2^n}\sum_{y\in 2^n}|y>\sum_{x\in 2^n}(-1)^{x.y}|f(x)>\end{aligned}$$

et on à $q_y = \sum_{x\in 2^n}(-1)^{x.y}|f(x)>$. Le claim c'est qu'on obtient un vecteur $v \in \mathbb{F}_2^n$ uniformément distribué orthogonal à a en sortie. Ça se voit direct en regardant $y.a \mod 2$:

$$q_y = \sum_{\bar{x}\in(\mathbb{Z}/2\mathbb{Z})^n/<a>}(1+(-1)^{a.y})((-1)^{x.y}|f(x)>$$

$$\begin{aligned}
a.y = 1 \mod 2 \to q_y &= \sum_{\bar{x} \in (\mathbb{Z}/2\mathbb{Z})^n/<a>} (1 + (-1)^{a.y})((-1)^{x.y}|f(x) > \\
&= 0 \\
a.y = 0 \mod 2 \to q_y &= \sum_{\bar{x} \in (\mathbb{Z}/2\mathbb{Z})^n/<a>} (1 + (-1)^{a.y})((-1)^{x.y}|f(x) > \\
&= \sum_{\bar{x} \in (\mathbb{Z}/2\mathbb{Z})^n/<a>} ((-1)^{x.y}|f(x) >
\end{aligned}$$

En particulier, y'a que les $y.a = 0 \mod 2$ qui ont une proba de sortir. L'uniforme distribution est claire.

Pour obtenir a, on peut lancer l'algorithme jusqu'à obtenir une base de $< a >^T$.

Remarque 1. *La proba d'avoir une base en m étapes se calcule bien, regarder la matrice des m vecteurs colonnes. Calculer sur le rang sur les lignes! On obtient une proba* $P_{d+k} \geq 1 - \frac{1}{q^k(q-1)} = 1 - \frac{1}{2^k}$ *avec* $q = 2$ *ici et* $d = n - 1 = dim < a >^T$.

1.4 Transormée de Fourier quantique

On a une nouvelle porte,

$$QFT(|x >) = \frac{1}{2^{n/2}} \sum_{y \in 2^n} \zeta_{2^n}^{x.y} |y > .$$

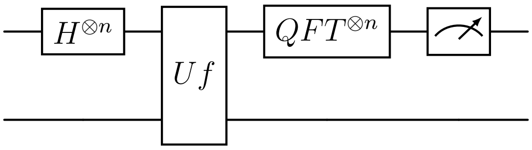
Et on peut l'utiliser pour trouver la période d'une fonction! Y'a une nuance dans la suite :

On part de $\mathbb{Z}/2^n\mathbb{Z}$ et pas $(\mathbb{Z}/2\mathbb{Z})^n$, puis xy est le produit dans $\mathbb{Z}/2^n\mathbb{Z}$ pas le produit scalaire.

Problème 1. $f : \mathbb{F}_2^n \to X$ telle qu'il existe $d \leq n$ t.q :

1. f est 2^d-périodique.
2. $f(x) = f(y)$ ssi $2^d \mid x - y$.

Le circuit



mesure un $|y>$ uniforme divisible par 2^{n-d}. En particulier, on a une manière de chopper une période de la forme 2^d en itérant. Donc en gros comme d'hab on regarde :

$$\sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} |x > |f(x) >$$

et on applique QFT cette fois pour obtenir :

$$\sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \sum_{y \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_{2^n}^{xy} |y > |f(x) >$$

et on pose

$$q_y = 1/2^n \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_{2^n}^{xy} |f(x) >$$

puis on écrit $x = a + 2^d b$, alors $f(x) = f(a)$. On peut montrer que

1. si $2^{n-d} \mid y$ alors $||q_y||^2 = 1/2^d$.
2. sinon $||q_y||^2 = 0$.

Fait : En gros, en prenant la QFT comme boite noire, j'ai revu deutsh josza et simon. Puis Shor pour trouver les périodes de la forme 2^k. Ensuite pour une période de la forme r générale, on peut l'estimer à partir du circuit du dessus. **À faire :** Comprendre l'estimation d'abord, via les fractions continues. Puis comprendre la QFT sans boite noire mais ca c'est moins important. Faut savoir construire $|x > \mapsto |0 > + \zeta_{2^n}^x |1 >$.