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 :

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

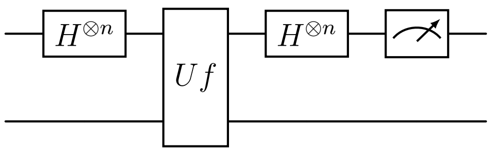
En particulier $||q_{0^n}|| = \sum_{x\in 2^n}(-1)^{f(x)}/2^n$. D'où si f est constant on obtient 0^n avec proba 1, sinon proba 0 d'avoir 0^n.

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.