Frédéric Magniez
Miklos Santha

DEA Algorithmique

Calcul quantique

Feuille n° 3 : Estimation de phase, algorithmes de recherche

Exercice 1

Soient $0 < \varphi < 1$ et $|\varphi_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2i\pi\varphi\times k}|k\rangle$. Soient F la transformée de Fourier quantique modulo 2^n, et $F^{-1}|\varphi_n\rangle = \sum_{y=0}^{2^n-1} \alpha_y|y\rangle$. Soit $a = a_1a_2\dots a_n$ la meilleure n-bit approximation de $2^n \times \varphi$.

Montrer que $|\alpha_a|^2 = \Theta(1)$.

Exercice 2

Soit $f : \{0,\dots,N-1\} \to \{0,1\}$ une fonction booléenne donnée par oracle quantique. Décrire un algorithme quantique qui détermine le plus petit $x \in \{0,\dots,N-1\}$ tel que $f(x) = 1$, et dont la complexité en requêtes à l'oracle est en $O(\sqrt{N})$.

Exercice 3

Soit $f : \{0,\dots,N-1\} \to \{0,1\}$ une fonction booléenne donnée par oracle quantique.

Avec la promesse $|f^{-1}(1)| = N/4$, donner un algorithme quantique exact qui trouve un élément $x \in \{0,\dots,N-1\}$ tel que $f(x) = 1$ en une seule requête à l'oracle.

Exercice 4

Soit $f : \{0,\dots,N\} \to \{0,1\}$ une fonction booléenne donnée par l'oracle $S_f(\varphi)|x\rangle = (e^{i\varphi})^{f(x)}|x\rangle$, pour un certain réel $0 \leq \varphi < 2\pi$ tel que $\varphi \neq \pi$.

- Expliquer comment implémenter $S_f(\varphi)$ à partir d'un oracle quantique calculant f.
- En supposant $|f^{-1}(1)| = N/2$, montrer que, pour une valeur de φ, il existe un algorithme quantique exact qui trouve l'unique élément $x \in \{0,1\}$ tel que $f(x) = 1$ en une seule requête à l'oracle.
  <u>Indication</u> : Etudier d'abord le cas $N = 2$ en reprenant l'opérateur de Grover $G = H \circ S_\delta \circ H \circ S_f$, dans lequel S_f est remplacé par $S_f(\varphi)$ et S_δ par $S_\delta(\psi)$, pour un certain réel ψ.
- Que faire pour $\varphi = \pi$?

Exercice 5

Soit $f : \{0,\dots,3\} \to \{0,1\}$ une fonction booléenne donnée par l'oracle quantique telle que $|f^{-1}(1)| \leq 1$.

Donner un algorithme quantique sans erreur, utilisant deux requêtes, et qui renvoie 0 si $|f^{-1}(1)| = 0$ et 1 sinon.

Montrer que la complexité de requêtes est optimale.

<u>Indication</u> : Procédér par l'absurde en considérant un algorithme quantique sans erreur et n'utilisant qu'une seule requête pour ce problème.
Soient $|\psi_0^f\rangle$ l'état quantique de l'algorithme avant l'appel à f, et $|\psi_1^f\rangle$ l'état après l'appel à f. Pour $k = 0,1$, soit $W_k = \sum_f |\langle\psi_k^{f_0}|\psi_k^f\rangle|$, où f_0 est la fonction partout nulle, et la sommation porte sur l'ensemble des fonctions $f : \{0,\dots,3\} \to \{0,1\}$ telles que $|f^{-1}(1)| = 1$.
Montrer alors que $W_0 = 4$, $W_1 = 0$, et $W_0 - W_1 \leq 2$. Conclure.