Frédéric Magniez
Miklos Santha

DEA Algorithmique

Calcul quantique

Feuille n° 2 : Circuits quantiques, calcul avec oracle

Exercice 1

Soit $f : \{0,1\}^n \to \{0,1\}^n$ une fonction donnée par un oracle quantique qui est ou bien une bijection, ou bien une fonction satisfaisant la promesse de Simon :

$$\exists u \in \{0,1\}^n - \{0^n\}, \quad \forall x,y \in \{0,1\}^n, \quad f(x) = f(y) \iff x = y \text{ ou } x \oplus y = u.$$

Spécifier un algorithme quantique efficace qui distingue ces deux cas.
Quel est le nombre de requêtes effectuées par votre algorithme ?

Exercice 2

Soient $f : \{0,1\}^n \to \{0,1\}^n$ et $g : \{0,1\}^n \to \{0,1\}^n$ deux bijections données par deux oracles quantiques telles que

$$\exists u \in \{0,1\}^n - \{0^n\}, \quad \forall x \in \{0,1\}^n, \quad f(x) = g(x \oplus u).$$

Donner un algorithme quantique qui détermine u.
Quel est le nombre de requêtes effectuées par votre algorithme ?

Exercice 3

Le but de cet exercice est de construire une solution quantique efficace dans le pire cas (et non en moyenne) et sans erreur au problème de Simon.

Soit $f : \{0,1\}^n \to \{0,1\}^n$ une fonction donnée par un oracle quantique satisfaisant la promesse de Simon pour un certain $u \in \{0,1\}^n$ tel que $u \neq 0^n$. Soit $H = \{h \in \{0,1\}^n : h \cdot u = 0\}$.

Pour tout ensemble $A \subseteq \{0,1\}^n$ et tout élément $g \in \{0,1\}^n$, on note

$$|\varphi_g A\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{g \cdot a} |a\rangle.$$

- Modifier l'algorithme de Simon tel qu'à chaque étape il renvoie un élément $y \in \{0,1\}^n$ tel que $y \neq 0^n$ et $y \in H$.
- Etant donnés $x \in H$ et i tel que $x_i = 1$, construire un circuit quantique qui prenant en entrée l'état $|\varphi_g H\rangle|0\rangle$, pour $g \in \{0,1\}^n$, renvoie l'état $|\varphi_g K\rangle|g \cdot x\rangle$, où $K = \{h \in H : h_i = 0\}$.
- Donner un algorithme quantique dans (F)EQP^f pour trouver u étant donnée f sous forme d'oracle quantique.
- Calculer la complexité en opérations et en requêtes de votre algorithme.

Exercice 4

Soit $C(p)$ l'arbre binaire uniforme de profondeur p. Cet arbre définit naturellement un circuit à $n = 2^p$ variables après avoir étiqueté des feuilles par les variables booléennes $x_1, \ldots, x_n$, et placé des portes NAND aux sommets internes. Soit $f : \{0,1\}^n \to \{0,1\}$ la fonction calculée par ce circuit.

- Montrer que la complexité de requête déterministe de f est n.

– Donner un algorithme probabiliste Las Vegas (sans erreur) de complexité inférieure à n pour ce problème.
– Quelle est la complexité exacte de votre algorithme?

Exercice 5

Soit $f : \{0,1\}^n \to \{0,1\}$ une fonction booléenne à n variables. Une assignation partielle est une fonction $C : S \to \{0,1\}$ pour une sous-ensemble $S \subseteq \{x_1, \ldots ,x_n\}$ des variables. La taille $|C|$ de C est la cardinalité de S. On dit que C est consistent avec $a \in \{0,1\}^n$, si $C(x_i) = a_i$ pour tout $x_i \in S$. Pour $b \in \{0,1\}$, un b-certificat pour f est une assignation partielle C telle que $f(a) = b$ pour tout $a \in \{0,1\}^n$ consistent avec C. La complexité de certificat $C_a(f)$ de f sur a est la taille du plus petit $f(a)$-certificat consistent avec a. La complexité de certificat de f est $C(f) = \max_a C_a(f)$. On dénote par $D(f)$ la complexité déterministe de requête de f.

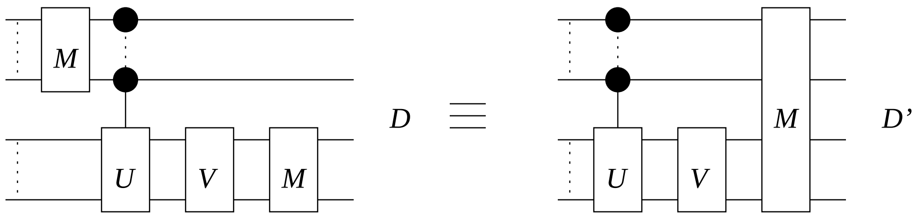
Montrer que pour chaque $f : \{0,1\}^n \to \{0,1\}$ on a

$$D(f) \leq C^2(f).$$

Exercice 6

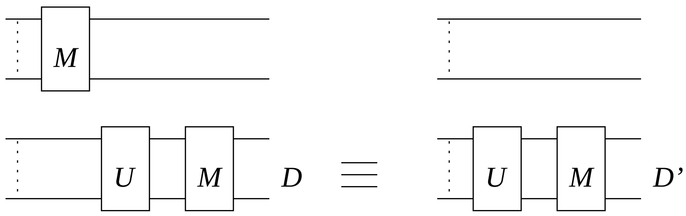
Mesure de contrôle

Montrer que Mesure et Control-U commutent (*i.e.* les distributions D et D' de la figure sont identiques) :



Mesure implicite

Montrer que si des qubits ne sont plus jamais utilisés dans un calcul, alors les mesurer ne change pas la distribution finale sur les autres (*i.e.* les distributions D et D' de la figure sont identiques) :



Exercice 7

Montrer que $\mathrm{BQP}^{\mathrm{BQP}} = \mathrm{BQP}$.