TD 2 - Algorithme de Grover et algorithme de Shor

Informatique quantique pour la recherche opérationnelle, S5.

2023

Exercice 1 — *Changeons deux-trois trucs* Dans cette exercice, on dispose d'une fonction f telle qu'il existe un unique $s \leq 2^n$ tel que $f(s) = 1$. On veut comprendre ce qu'il se passe si on modifie un peu l'entrée de l'algorithme de Grover.

1. Que se passe-t-il si, au lieu de donner $|\underline{0}\rangle$ on donne $-|\underline{0}\rangle$ au circuit de l'algorithme de Grover? S'approche-t-il de la solution ? Si oui, en combien d'itérations ? Si non, comment corriger l'algorithme ?

2. On suppose que $s > 1$. Mêmes questions si on démarre de $H^{\otimes n}(|\underline{0}\rangle - |\underline{1}\rangle)$.

Exercice 2 — *Amplification quantique*

Soit une fonction $f : \{0,1\}^n \to \{0,1\}$ telle qu'il existe un unique s tel que $f(s) = 1$. Soient $\varepsilon > 0$ et un algorithme probabiliste A qui, avec une probabilité supérieure à ε, renvoie s. On cherche à construire un algorithme B qui renvoie s avec une probabilité supérieure à $\frac{2}{3}$.

Partie 1. Amplification

1. (a) Soit $k \in \mathbb{N}$ et B l'algorithme qui appelle k fois l'algorithme A. Il renvoie s si au moins une des occurences de A a renvoyé s. Quelle est la probabilité que B renvoie s ?

   (b) En déduire la valeur de k nécessaire pour que cette probabilité dépasse $\frac{2}{3}$.

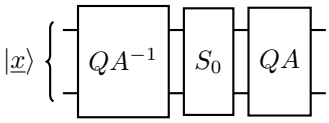
2. On dipose maintenant d'un circuit quantique QA de A. Cet algorithme a la propriété suivante: $QA\,|\underline{0}\rangle$ renvoie $\sum_{x=0}^{2^n-1} a_x\,|\underline{x}\rangle$. On suppose $a_x \in \mathbb{R}^+$. Enfin, on suppose $|a_s|^2 \geq \varepsilon$. On suppose a_s et ε petits.

   (a) Quelle est la probabilité qu'on mesure s à l'issue de ce circuit?

   (b) Quel est l'angle entre le vecteur $QA\,|\underline{0}\rangle$ et $\sum_{x \neq s} a_x\,|x\rangle$?

   (c) Quel est l'angle entre le vecteur $QA\,|\underline{0}\rangle$ et $|s\rangle$?

   (d) Que fait le circuit suivant où S_0 est la symétrie par rapport à $|\underline{0}\rangle$?



   (e) Proposez un circuit qui permet de mesurer l'état cible avec une probabilité au moins $\frac{2}{3}$. Combien de fois l'algorithme QA est appelé par ce circuit ?

Partie 2. Collision

On supposera que l'amplification précédente fonctionne également si s n'est pas unique.

On dispose d'une fonction $H : 0,1^n \to 0,1^n$. On cherche x et y tels que $H(x) = H(y)$ et $x \neq y$ (on dit qu'il y a collision). On suppose que, pour tout x, il existe une collision avec au moins un autre y.

On fixe un entier k. On applique l'algorithme suivant:

- Evaluer et trier $H(x)$ pour $x < k$.
- Vérifier s'il y a collision.
- Sinon, choisir y entre k et $2^n - 1$ et répondre OUI si $H(y) = H(x)$ pour $x \leq k$.

1. Quelle est la probabilité de succès de cet algorithme?
2. Proposez un algorithme quantique qui trouve une collision avec une forte probabilité en $O(\sqrt[3]{2^n})$ appels à H.

Exercice 3 — *Exemple d'exécution de l'algorithme de Shor*

Quelles sont les exécutions possibles de l'algorithme de Shor quand on cherche à factoriser 91 ?