TD3 — Algorithme de recherche de Grover

Ex1 Soit $f: \{0,1\}^n \to \{0,1\}$ réalisée par un circuit quantique $U_f: |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$.

- (a) Montrer par le calcul que $U_f: |x\rangle |-\rangle \mapsto (-1)^{f(x)} |x\rangle |-\rangle$.
- **(b)** Construire un circuit $Z_{\text{OR}}: |x\rangle |0\rangle \mapsto (-1)^{\text{OR}(x)} |x\rangle |0\rangle$ où OR est le OU à n entrées.

Ex2 La clé de voûte de l'algorithme de Grover est l'opérateur $G=2\left|0\right>^{\otimes n}\left<0\right|^{\otimes n}-I_n$.

- (a) Calculer la matrice de $|0\rangle^{\otimes n} \langle 0|^{\otimes n}$ puis celle de G.
- (b) Montrer que le circuit Z_{OR} de l'exercice précédent calcule G .

Ex3 L'opérateur de diffusion de Grover est $M = H^{\otimes n}GH^{\otimes n}$.

- (a) Calculer $|u\rangle = H^{\otimes n} |0\rangle^{\otimes n}$.
- **(b)** Montrer que $M = 2 |u\rangle \langle u| I$.
- (c) Développer $|u\rangle\langle u|$.
- (d) Montrer que $M: \sum_k c_k |k\rangle \mapsto \sum_k (2\langle c \rangle c_k) |k\rangle$ où $\langle c \rangle = \frac{1}{2^n} \sum_k c_k$.
- (e) Discuter de l'interprétation de ce calcul comme une opération miroir autour de la moyenne.

Ex4 On se place tout d'abord dans le cas où la fonction f ne prend qu'une seule fois la valeur 1. Décrire la construction complète du circuit de Grover : initialisation, étapes de calcul, nombre optimal d'étapes.

- (a) Décrire complétement le circuit pour 2 qubits puis calculer la probabilité d'obtenir le résultat.
- **(b)** Recommencer avec un unique qubit!
- (c) Estimer le nombre total de portes et la profondeur du circuit en fonction du nombre de qubits.

Ex5 Rappeler l'algorithme vu en cours pour le cas général où f admet un nombre quelconque de solutions. Quelle est la probabilité de trouver une solution après une exécution? Expliquer comment adapter l'algorithme pour garantir de trouver une solution avec probabilité au moins 1-1/N. Estimer la complexité en temps totale de l'algorithme.