1 TD 2. Calcul quantique : bases et algorithme de Grover

Rappels du cours

1. Donnez la représentation matricielle de l'ensemble universelle des portes logiques quantiques qu'on utilisera dans la suite : Hadamard, $S(\pi/4)$, C-NOT. Les premières sont portes à un seul qubit et la troisième est une porte à deux qubit. Quelle est leur action sur la base de calcul $|j_1\rangle|j_2\rangle$ avec $j_i = \{0, 1\}$?

2. Rappeler la définition de parallélisme quantique.

3. Quel genre d'opérateur est-il l'oracle dans l'algorithme de Grover (hermitique, unitaire,...) ? Quelle est son action sur la base $|x\rangle|q\rangle$ où $|x\rangle$ est un registre de donnée à n qubits $|q\rangle$ est un registre de résultat à un seul qubit ?

4. Quel est l'autre opération unitaire necessaire pour implémenter l'algorithme de Grover sur une base de données ?

5. Quelle est la complexité de l'algorithme de Grover sur une base de données comprenante N éléments non triés, non liés, numérotés de 0 à $N-1$? De combien de tirages classiques on aurait besoin pour trouver l'élément cherché x_0 ?

2 Parallélisme quantique

Exercice 2.1: Operateur AND, réversibilité et qubit auxiliaire L'opérateur AND n'est pas inversible $(x, y) \to f(x, y) = x \wedge y = xy$ (rappeler la table de verité). On peut la mettre en oeuvre de façon réversible en utilisant une variable auxiliaire $(x, y, z) \to f(x, y, z)$. Quelle est la porte classique que nous le permettrait ? Donner la représentation matricielle de l'opérateur unitaire U_f correspondent à cette porte dans l'espace des états à $2^{2+1} = 8$ dimensions.

Exercice 2.2: Fonctions de $\{0, 1\}$ dans $\{0, 1\}$ Il existe 4 fonctions de $\{0, 1\}$ dans $\{0, 1\}$ listées ci-dessous : f_0 et f_3 sont les fonctions constantes et f_1 et f_2 sont respectivement la fonction identité et la fonction NOT ; Ces deux dernières sont des fonctions équilibrées.

$$\begin{array}{ccc} x & 0 & 1 \\ -- & -- & -- \\ f_0(x) & 0 & 0 \\ f_1(x) & 0 & 1 \\ f_2(x) & 1 & 0 \\ f_3(x) & 1 & 1 \end{array} \tag{1}$$

— Pour chacune de ces fonctions construire la matrice unitaire U_f qui implémente $(x, y) \to (x, y \oplus f(x))$

— Trouver l'état résultant de l'application de la transformation U_{f_2} (NOT) à l'état $(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|10\rangle$ puis à l'état $(\alpha|0\rangle + \beta|1\rangle)|1\rangle = \alpha|01\rangle + \beta|11\rangle$; on pourra utiliser soit la représentation matricielle soir la définition ci-dessus.

3 Algorithme de Grover

Exercice 3.1: Dans cet exercice on détaillera l'algorithme de Grover vu en cours.

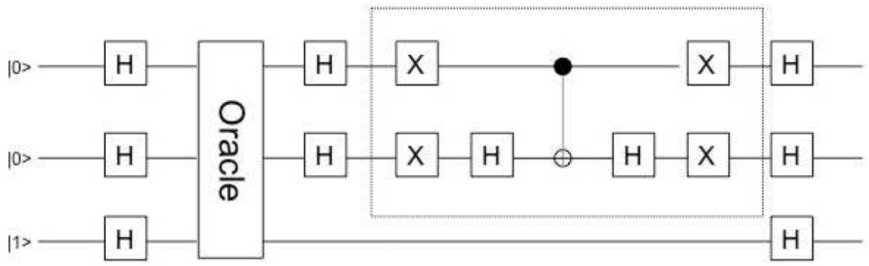

FIGURE 1 – Circuit Grover

1. Montrer que l'opération $S_\psi = 2|\psi\rangle\langle\psi| - I$ réalise dans le plan $(|\alpha\rangle, |x_0\rangle)$ une symétrie par rapport à la direction de l'état $|\psi\rangle$; *Indication : Introduire un vecteur* $|\Phi\rangle$ *du plan* $(|\alpha\rangle, |x_0\rangle)$ *qui soit orthogonal à* $|\psi\rangle$. Rappeler la représentation géométrique de l'algorithme.
2. Probabilité d'erreur
   - Quel est le nombre optimal d'itérations ?
   - Quand on réalise la mesure à ce moment là quelle est la probabilité de ne pas trouver $|x_0\rangle$?
3. On va mettre en oeuvre l'algorithme de Grover dans le cas d'une liste de 4 éléments : on a donc $N = 4$ et $n = 2$; le registre comportera donc deux qubits.

   - Montrer que dans le cas où $x_0 = 3$ le circuit associé à la porte de Toffoli fait fonction d'oracle $|x\rangle|q\rangle \to |x\rangle|q \oplus f(x)\rangle$ cad que $f(3) = 1$ et $f(x) = 0$ sinon.

   - Montrer que le circuit ci-dessus (Fig. 1) permet de trouver x_0 en exactement une itération (on prendra $x_0 = 3$).