Homework 4
Traitement Quantique de l'Information

Exercice 1 *Algorithme de Deutsch et Josza le plus simple possible*

On considère une fonction d'un bit classique $f(x)$ qui prend ses valeurs dans $\{0,1\}$. Il existe 4 fonctions de ce type. On veut déterminer si la fonction est constante ou balancée (il y a deux fonctions constantes et deux fonctions balancées). Avec un "circuit classique" pour déterminer si f est constante ou balancée il faut calculer les deux sorties possibles $f(0)$ et $f(1)$ puis les comparer (par exemple on calcule $f(0)-f(1)$ et on détermine si cette différence vaut 0 ou 1). On doit "appeler" la fonction f deux fois.

On suppose que l'on a disposition une porte quantique qui effectue l'opération

$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

a) Montrez que U_f est une matrice unitaire.

b) Reprendre le circuit de Deutsch et Josza du cours et refaire l'analyse détaillee dans ce cas particulier. Montrez en particulier qu'une seule utilisation du circuit suffit à déterminer si f est constante ou balancée.

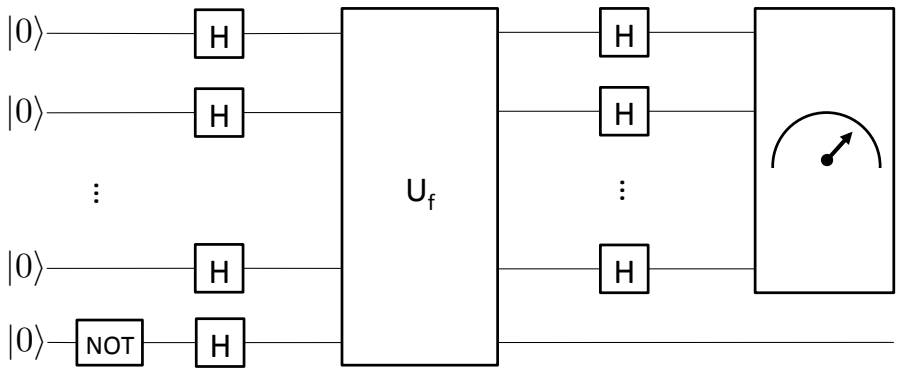
Exercice 2 *Algorithme de Bernstein-Vazirani*

En 1993 E. Bernstein et U. Vazirani (Proc, 25th Annual ACM Symposium on the Theory of Computing, ACM Press, NY p11-20) formulèrent le problème suivant.

Soit $\underline{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$ des vecteurs binaires à n composantes. On se donne un "oracle" qui calcule

$$f(\underline{x}) = b \oplus (\underline{a} \cdot \underline{x}) \mod 2$$

où $b \in \mathbb{F}_2$ et $\underline{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_2^n$ et $\underline{a} \cdot \underline{x} = \sum_{i=1}^n a_i x_i$. Le but est de calculer $\underline{a}$ en posant le moins de questions possibles à l'oracle : pour fixer les idées on suppose b connu et $\underline{a}$ inconnu. On considère le circuit de Deutsch et Josza :



Rappel : $U_f|x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |y\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |y \oplus f(\underline{x})\rangle$

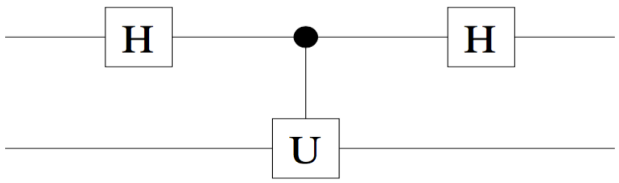
a) Calculez l'état de sortie du circuit - juste avant l'appareil de mesure - quand tous les qubits d'entrée sont dans l'état $|0\rangle$. Il est utile de remarquer que $|f(\underline{x})\rangle - |1 \oplus f(\underline{x})\rangle = (-1)^{f(\underline{x})}(|0\rangle - |1\rangle)$.

b) Grâce à l'appareil de mesure on fait *une seule* mesure dans la base computationelle des n premiers qubits de sortie du circuit. Montrer que cela suffit à déterminer le vecteur $\underline{a}$ avec probabilité 1.

c) A-t-on besoin de savoir la valeur de b pour le succès de l'algorithme ? Si celle-ci n'est pas connue, est-ce que cet algorithme permet de la déterminer ? Justifiez.

Exercice 3 *Un petit algorithme quantique*

Soit U une matrice unitaire et $|u\rangle$ un vecteur propre, c'est à dire $U|u\rangle = \exp(2\pi i\varphi)|u\rangle$. Considérez le circuit suivant :



a) Calculez la sortie pour l'état initial $|0\rangle \otimes |u\rangle$.

b) Calculez la probabilité d'observer le premier bit dans l'état $|0\rangle$ à la sortie. Même question pour la probabilité d'observer le premier bit dans l'état $|1\rangle$ à la sortie.

c) Supposons que l'on remplace U par U^k, k entier dans le circuit ci-dessus. Soit $\varphi = 0, \varphi_1\varphi_2...\varphi_t$ ou $\varphi_i \in \{0, 1\}$ le développement binaire de $0 < \varphi < 1$. En d'autres termes $\varphi = \frac{\varphi_1}{2} + \frac{\varphi_2}{2^2} + \cdots + \frac{\varphi_t}{2^t}$. Comment choisir k pour déterminer le bit le moins significatif φ_t en une seule mesure ? *Indication* : inspirez vous de la question b).