Exercise Set 5 : 24 March 2016
Calcul Quantique

Exercise 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

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

Montrez que U_f est une matrice unitaire.

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 de U_f suffit à déterminer si f est constante ou balancée.

Exercise 2 *Vérifications pour bonne compréhension si besoin est.*

a) On adopte la notation $|b\rangle$, $|c\rangle$ pour les états de la base canonique (c.a.d que $b = 0, 1$ et $c = 0, 1$) $|0\rangle$, $|1\rangle$. Vérifiez

$$H|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) = \frac{1}{\sqrt{2}}\sum_{c=0}^{1}(-1)^{bc}|c\rangle$$

et vérifiez pour $n = 2$ et 3

$$H^{\otimes n}|0_n\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{(b_1\ldots b_n)\in\mathbb{F}_2^n}|b_1, ..., b_n\rangle$$

$$H^{\otimes n}|b_1, ..., b_n\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{(c_1\ldots c_n)\in\mathbb{F}_2^n}(-1)^{\sum_{i=1}^{n} b_i c_i}|c_1, ..., c_n\rangle$$

et ensuite le cas général.

b) Détaillez les algorithmes de Deutsch-Josza (cours) et Bernstein-Vazirani (série 2) pour $n = 2$. Reprendre le cas général.

Exercise 3 *Variation sur le problème de Deutsch-Josza*

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. On se donne un "oracle" qui calcule

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

pour chaque entrée $\underline{x} \in \mathbb{F}_2^n$. Ici $\underline{a} \in \mathbb{F}_2^n$ et $b \in \mathbb{F}_2$. Le but est de calculer $\underline{a}$ en posant le moins de questions possibles à l'oracle.

1. Combien de questions faut-il poser à l'oracle pour déterminer $\underline{a}$ classiquement ?
2. Montrez que
$$\sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{\underline{x} \cdot \underline{z}} = \begin{cases} 2^n & \text{si } \underline{z} = (0, 0, ..., 0) \\ 0 & \text{sinon} \end{cases}$$
3. En utilisant le point précédent montrez que grâce au circuit de Deutsch-Josza, il suffit de poser une seule question à "l'oracle quantique" pour déterminer $\underline{a}$.