Exercise Set 5 : 21 March 2018
Calcul Quantique

Exercise 1 *Algorithme de Simon*

Il s'agit de réfléchir aux calculs du cours dans un cas très concret. On considère le sous espace vectoriel de dimension 1

$$H = \{(0,0);(1,0)\}$$

"caché" dans le carré binaire

$$\mathbb{F}_2^n = \{(0,0);(1,0);(1,0);(1,1)\}$$

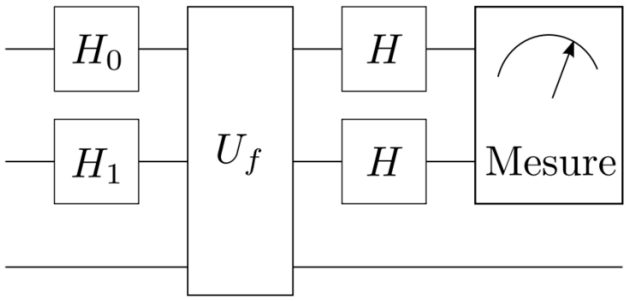
En d'autre termes on dispose d'un oracle qui retourne deux valeurs distinctes pour une fonction $f : \mathbb{F}_2^n \to X$ (où X possède deux éléments) telle que $f(x_1, x_2) = f(y_1, y_2)$ si et sulement si $(x_1, x_2) = (y_1, y_2)$ ou $(x_1, x_2) - (y_1, y_2) = (1, 0)$. le but est de trouver le vecteur $(1, 0)$ (c'est le vecteur de base du sous-espace caché H).

Exercise 2 *Effet des imperfections sur l'algorithme de Simon*

On considère le problème de Simon pour $n = 2$. Soit $H = \left\{\underline{x} \in \mathbb{F}_2^2 \;\middle|\; \underline{x} = (0, x_2), \text{avec } x_2 \in \{0,1\}\right\}$. C'est le "sous-espace vectoriel caché" de $\mathbb{F}_2^2$. Soit $f : \mathbb{F}_2^2 \longrightarrow \{0,1\}$ telle que $f(\underline{x}) = f(\underline{y})$ si et seulement si $\underline{x} - \underline{y} \in H$.

Pour fixer les idées on prendra la fonction $f(0,0) = f(0,1) = 0$ et $f(1,0) = f(1,1) = 1$.

Considérez le circuit (de l'algorithme de Simon) :



où H_0 et H_1 sont des portes de Hadamard *imparfaites* :

$$H_0 |b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b e^{i\phi_0} |1\rangle\right)$$
$$H_1 |b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b e^{i\phi_1} |1\rangle\right)$$

et ϕ_0 et ϕ_1 sont des phases dans $[0, 2\pi]$. Les deux dernières portes du circuit sont des portes de Hadamard standard

$$H\left|b\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + (-1)^b\left|1\right\rangle\right)$$

et $U_f\left|x_1, x_2\right\rangle \otimes \left|z\right\rangle = \left|x_1, x_2\right\rangle \otimes \left|z \oplus f(x_1, x_2)\right\rangle$. Le circuit est initialisé à $\left|0, 0\right\rangle \otimes \left|0\right\rangle$.

1. Calculez l'état juste après les deux premières portes de H_0 et H_1.
2. Calculez l'état après U_f, puis enfin calculez l'état juste après les deux dernières portes de Hadamard (c.à.d. juste avant la mesure).
3. On mesure les deux premiers qu-bits dans la base définie par les projecteurs

$$\left\{\left|\underline{y}\right\rangle\left\langle\underline{y}\right| \otimes I \;\middle|\; \underline{y} \in \{00, 01, 10, 11\}\right\}.$$

   Le qu-bit de stockage n'est pas mesuré, ce qui est reflété par la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   Calculez les probabilités d'obtenir les états $\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle, \left|11\right\rangle$ juste après la mesure.
4. Déduire la probabilité de tomber sur un vecteur de $H^\perp$ et celle de tomber sur un vecteur de H. Pour quelles valeurs de ϕ_0 et ϕ_1 retrouve-t-on les cas où les portes de Hadamard sont parfaites ? Y a-t-il quelque chose d'étonnant dans vos résultats ?