Exercice 1  Effet des "imperfections" sur quelques portes dans l'algorithme de Shor

On considère une fonction sur $\mathbb{Z}$, de période égale à 2. C'est à dire $f(x) = f(x+2)$, $x \in \mathbb{Z}$. Nous voulons étudier le circuit ci-dessous (voir figure) où les portes de Hadamard usuelles sont modifiées par une perturbation aléatoire

$$\tilde{H}_0 |b\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + (-1)^b e^{i\varphi_0} |1\rangle \right), \text{ où } b = 0, 1$$

$$\tilde{H}_1 |b\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + (-1)^b e^{i\varphi_1} |1\rangle \right), \text{ où } b = 0, 1$$

avec $\varphi_0$ et $\varphi_1$ uniformément distribués sur $[0, 2\pi]$.

Le circuit est initialisé dans l'état $|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle$. On prendra la convention $|0\rangle \otimes |0\rangle = |0\rangle$ ; $|0\rangle \otimes |1\rangle = |1\rangle$ ; $|1\rangle \otimes |0\rangle = |2\rangle$ ; $|1\rangle \otimes |1\rangle = |3\rangle$ et les définitions pour $x, y \in \mathbb{Z}$ :

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

$$\text{QFT} |x\rangle = \frac{1}{\sqrt{4}} \sum_{y=0}^{3} \exp \left( \frac{2\pi i}{4} xy \right) |y\rangle$$
a) Montrez que l'état après les portes de type Hadamard est :

$$|\psi_1\rangle = \frac{1}{\sqrt{4}} \left( |0\rangle + e^{i\varphi_1} |1\rangle + e^{i\varphi_0} |2\rangle + e^{i(\varphi_0+\varphi_1)} |3\rangle \right) \otimes |0\rangle$$

b) Montrez que l'état juste avant la mesure est

$$|\psi_2\rangle = \frac{1}{4} \sum_{y=0}^{3} \left( 1 + e^{i(\varphi_0+\pi y)} \right) |y\rangle \otimes |f(0)\rangle + \left( e^{i(\varphi_1+\frac{\pi}{2} y)} + e^{i(\varphi_0+\varphi_1+\frac{3\pi}{2} y)} \right) |y\rangle \otimes |f(1)\rangle$$

c) On mesure les deux premiers qu-bit dans la base définie par les projecteurs

$$\{ P_y \otimes I_{4 \times 4} = |y\rangle \langle y| \otimes I_{4 \times 4}; \ y = 0, 1, 2, 3 \}$$

Calculez l'état juste après la mesure (a un facteur de normalisation près). Ensuite calculez la probabilité d'obtenir $y$. Vous devrez trouver un résultat indépendant de $\varphi_1$.

d) Dans la question précédente vous avez calculé une probabilité étant donné $\varphi_0$ et $\varphi_1$ fixés. En principe vous avez trouvé un résultat dépendant uniquement de $\varphi_0$. Faire un dessin de $Pr(y|\varphi_0)$ pour $\varphi_0 = 0, \frac{\pi}{2}, \frac{3\pi}{2}, \pi$. Calculez et dessinez la probabilité totale $Pr(y)$ en considérant que $\varphi_0$ est distribuée uniformément sur $[0, 2\pi]$.

**Exercice 2** Période d'une fonction et factorisation de $N = 15$

On veut factoriser le nombre $N = 15$ grâce à l'algorithme aléatoire vu en cours. Pour cela on tire un nombre $a$ au hasard dans $\{2, 3, ..., 15\}$. Nous supposerons que nous avons tiré $a = 7$ qui est premier avec 15.

a) Calculez l'ordre $\text{Ord}(7)$ c.à.d. le plus petit entier $r$ tel que $7^r = 1 \mod 15$. Pour cela vous calculerez les premières valeurs de la fonction $f : x \rightarrow f(x) = 7^x \mod 15$.

b) Explicitier les étapes ultérieures de l'algorithme classique.

c) On veut maintenant expliciter l'algorithme quantique pour la recherche de l'ordre. Prendre le circuit quantique pour la période de la fraction $f : x \rightarrow (7^x \mod 15)$ avec $M = 2^{11} = 2048$.

**c1** Donnez l'état juste après les portes de Hadamard.

**c2** Donnez l'état juste après le circuit de $U_f$.

**c3** Donnez l'état après la QFT.

**c4** Montrez que $Pr(y)$ vaut $\frac{1}{4}$ si $y = 0, 512, 1024$ et 1536 et vaut 0 sinon.

**c5** Supposons que la mesure nous donne le nombre $y = 1536$. Peut-on trouver $r$?

**c6** Même question si la mesure donne $y = 0, 512, 1024$ (discuter tous les cas!)

**Indications générale** : on pourra reprendre les formules générales du cours.

**Exercice 3** Remarques sur la transformée de Fourier Quantique et notamment son unitarité.

a) Montrer que pour $M = 2$ la transformation QFT n'est rien d'autre qu'une porte de Hadamard $H$.

b) Écrire explicitement $QFT |x\rangle$ pour $M = 4$ et $x = 0, 1, 2, 3$.

c) Montrer dans le cas général que QFT est une matrice unitaire. Indication : montrer que

$$\langle x' | (QFT) \dagger QFT |x\rangle = \langle x' | x \rangle$$