# Série 7
# Traitement quantique de l'information II

**Exercice 1** *Algorithme de Grover pour $N = 4$*

Soit $x \in \{x_0, x_1, x_2, x_3\}$ et $f(x) = 1$ si et seulement si $x = x_0$. Sinon $f(x) = 0$. On recherche $x_0$ grâce à un oracle qui retourne la valeur de $f$ quand on lui présente une entrée.

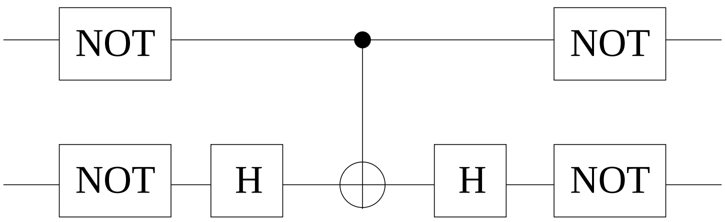
1. Montrez que le nombre moyen de questions à poser à un oracle classique, quand on présente les entrées uniformément aléatoirement et sans remise, est $2,25$.
2. D'après la théorie, quelle est le nombre de questions à poser à l'oracle quantique si on utilise le circuit de Grover ?
3. Dans le circuit de Grover on utilise l'opérateur suivant :

$$\mathbb{I} - 2\underbrace{|00...0\rangle}_{n \text{ fois}}\langle 00...0|$$

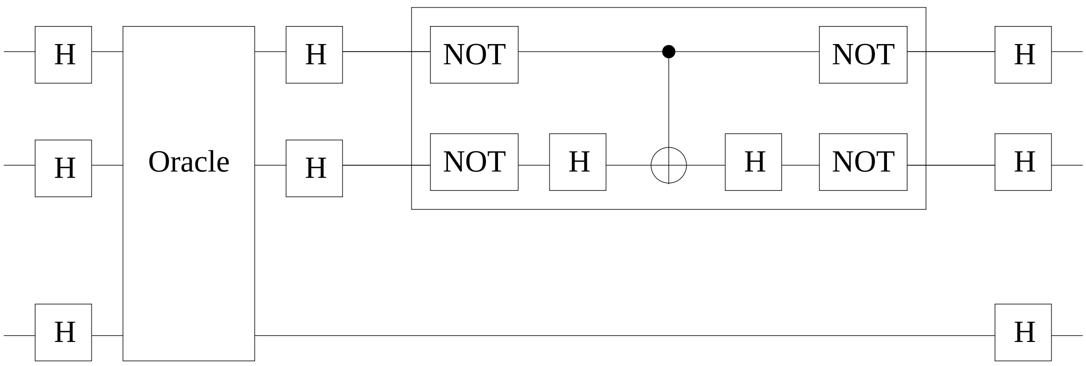
   Remarquez que cet opérateur agit comme :

$$\begin{aligned} &|00...0\rangle \to -|00...0\rangle \\ &|b_1 b_2 ... b_n\rangle \to |b_1 b_2 ... b_n\rangle \ \text{ si } \ (b_1 b_2 ... b_n) \neq (00...0) \end{aligned}$$

   Montrez que pour $n = 2$ (le cas présent) cet opérateur peut être réalisé par le circuit suivant :

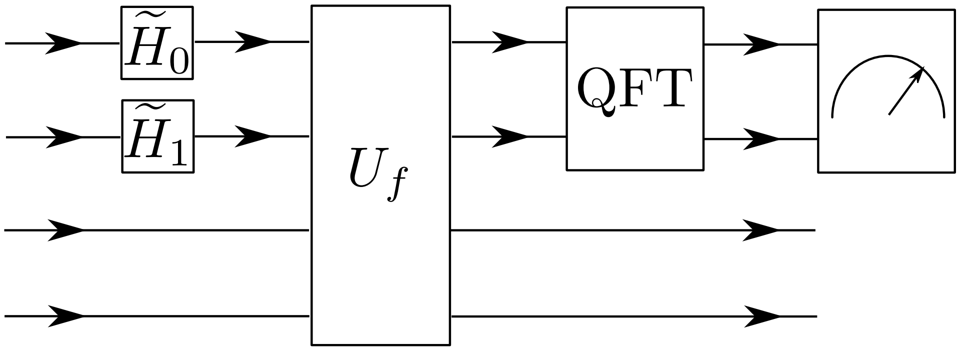



4. Prenez le circuit de l'algorithme de Grover pour $N = 4$ et donnez l'état quantique à chaque étape. Faites une représentation géométrique de l'état (dans un espace à 2 dimensions approprié). Confirmez que l'état final donne bien la réponse $x_0$ voulue et que l'on a posé une seule question à l'oracle.



**Exercice 2** *Effet de la décohérence 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 suivant :




où les portes de Hadamard usuelles sont modifiées par une perturbation aléatoire

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

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

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 $x, y \in \mathbb{Z}$ :

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

$$\text{QFT} |x\rangle = \frac{1}{\sqrt{4}} \sum_{y=0}^{3} \exp\left( \frac{2\pi i}{4} xy \right) |y\rangle$$

1. Montrez que l'état après les portes de type Hadamard est :

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

2. Montrez que l'état juste avant la mesure est

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

3. On mesure les deux premiers qu-bit dans la base définie par les projecteurs

$$\{ P_y \otimes \mathbb{I}_{4\times4} = |y\rangle \langle y| \otimes \mathbb{I}_{4\times4};\ y = 0, 1, 2, 3 \}$$

   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 $\varphi_1$ .

4. 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 $\varphi_0 = 0, \frac{\pi}{2}, \frac{3\pi}{4}, \pi$. Calculez et dessinez la probabilité totale $\Pr(y)$ en considérant que $\varphi_0$ est distribuée uniformément sur $[0, 2\pi]$.

5. Dans une expérience de RMN (imaginaire) quels sont les cas dans la question 4 ci-dessus qui permettent d'obtenir la période de $f$ ?