

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.

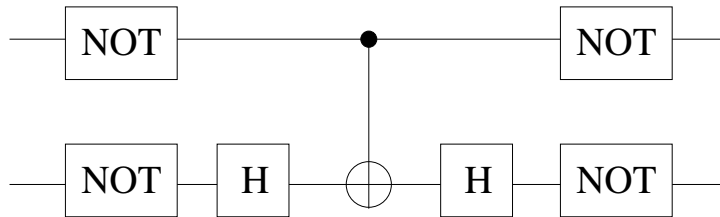
1. Quel est le nombre moyen de questions à poser à un oracle classique, quand on présente les entrées uniformément aléatoirement et sans remise ?
2. D'après la théorie, quelle est le nombre de questions à poser à l'oracle quantique si on utilise le circuit de Grover ?
3. Dans le circuit de Grover on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

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

Remarquez que cet opérateur agit comme :

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

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.

