# Exercices
# Semaine 5

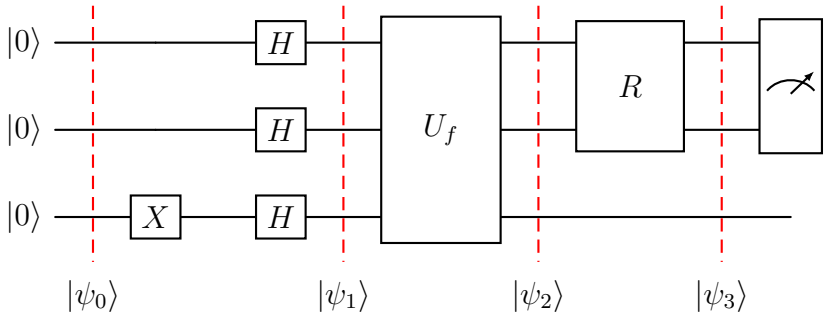
Cours Turing+

## 1 Circuit de réflexion pour l'algorithme de Grover

Soit $f : \{0,1\}^2 \to \{0,1\}$ une fonction booléenne telle que $f(x_0, y_0) = 1$ pour une seule valeur de $(x_0, y_0) \in \{0,1\}^2$.

**a)** Construire la porte oracle $U_f$ lorsque $x_0 = y_0 = 0$.

Le circuit de Grover permettant de trouver la valeur de $(x_0, y_0)$ avec une seule évaluation de l'oracle $U_f$ est alors le suivant :




où $R$ est le circuit de réflexion autour de l'état $|\psi_1\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} |x,y\rangle$ [1], que nous allons maintenant construire (*Note :* Tout ce qui suit est passablement guidé... Sentez-vous libres de d'abord réfléchir à comment construire ce circuit sans lire toutes les indications qui suivent).

**b)** Considérons tout d'abord le circuit $R_0$ permettant d'effectuer une réflexion autour de $|0,0\rangle$. Prenez un moment pour vérifier que $R_0$ doit satisfaire les relations suivantes :

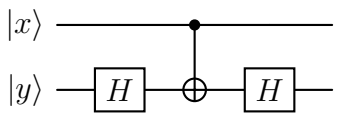
$$R_0 |0,0\rangle = |0,0\rangle \quad \text{et} \quad R_0 |x,y\rangle = -|x,y\rangle \quad \text{pour tout } (x,y) \neq (0,0)$$

et ainsi que $R_0$ est donné par la formule

$$R_0 = 2 |0,0\rangle \langle 0,0| - I$$

[1] Notez ici un petit abus de notation: on appelle $|\psi_1\rangle$ l'état composé des deux premiers qubits de l'état $|\psi_1\rangle$.

**c)** Rappelez-vous ensuite le circuit de l'exercice 2.a) de la série 2 :




La sortie de ce circuit vaut $(-1)^{xy}\,|x,y\rangle$. Il multiplie donc par $-1$ le seul état $|1,1\rangle$. A partir de là, construisez un circuit qui multiplie par $-1$ le seul état $|0,0\rangle$. Ce nouveau circuit est donc, à un signe global près, le circuit désiré $R_0$ (et notez qu'un signe global n'est pas un problème, car tous les états sont multipliés par le même signe, ce qui n'influence en rien la mesure finale).

**d)** En notant finalement que $|\psi_1\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} |x,y\rangle = H\,|0\rangle \otimes H\,|0\rangle$, nous pouvons en déduire, en utilisant la formule ci-dessus, que

$$R = (H \otimes H)\, R_0\, (H \otimes H)$$

ce qui permet de construire le circuit de réflexion $R$.

**e)** Testez finalement la sortie du circuit de Grover pour la porte $U_f$ vue au point a).

# 2 Plus difficile, maintenant...

Considérons la fonction booléenne $f : \{0,1\}^3 \to \{0,1\}$ définie par

$$f(x,y,z) = (x \text{ OR } y) \text{ AND } (\overline{x} \text{ OR } z) \text{ AND } (\overline{y} \text{ OR } \overline{z})$$

Construisez le circuit de Grover qui permet de trouver un état $|x,y,z\rangle$ tel que $f(x,y,z) = 1$.

*Trois points d'attention :*

- La construction de la porte $U_f$ peut se faire directement à partir de la définition de la fonction $f$, mais notez que celle-ci est donnée en termes de portes NOT, OR et AND, alors que vous ne pouvez utiliser que des portes NOT, CNOT et CCNOT (*indication :* voire CCCNOT ici !).

- Il faut aussi généraliser la porte $R$, car celle-ci prend maintenant trois qubits en entrée et en sortie, et non deux.

- A priori, on ne connaît pas le nombre de solutions $M$ ici (à moins de les calculer de manière classique, ce qu'on voudrait éviter). En pratique, il est possible d'y aller un peu "à l'aveuglette" et de tester le circuit de Grover avec 1, 2, 3,... rotations et voir ce qui fonctionne !