Notes de cours
Semaine 4

Cours Turing+

1 Problème de Deutsch-Josza

Ce problème est une généralisation du problème de Deutsch vu la semaine dernière. Soit $f : \{0,1\}^n \to \{0,1\}$ une fonction booléenne *dont on sait à l'avance* qu'elle est

- soit constante : $f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ pour tous $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \{0,1\}^n$

- soit balancée : $f(x_1, \ldots, x_n) = \begin{cases} 1 & \text{pour la moitié des points } (x_1, \ldots, x_n) \in \{0,1\}^n \\ 0 & \text{pour l'autre moitié} \end{cases}$

(*Exemple* de fonction balancée pour $n = 2$: $f(0,0) = f(1,1) = 1$ et $f(0,1) = f(1,0) = 0$)

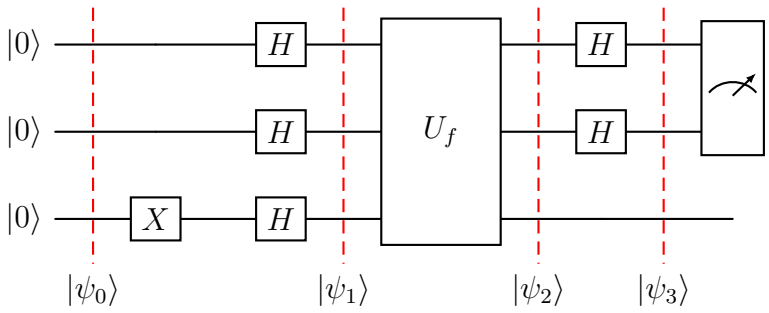
Le problème de Deutsch-Josza consiste à décider si f est une fonction constante ou balancée, ceci en effectuant un nombre minimum d'évaluations de la fonction f.

Classiquement, dans le pire des cas, il faut évaluer $f(x_1, \ldots, x_n)$ en $2^{n-1}+1$ valeurs différentes de $(x_1, \ldots, x_n)$ pour répondre à cette question. En effet, si f est constante, toutes les évaluations de f donneront la même réponse (soit 0, soit 1), et ce n'est donc qu'après avoir évalué f en plus de la moitié des points que nous pourrons être sûrs que f n'est pas une fonction balancée. Le nombre nécessaire d'évaluations de f est donc exponentiel en n dans ce cas.

Avec un circuit quantique, il est possible de répondre à cette question avec *une seule* évaluation de la fonction f, comme nous allons le voir.

Remarque : Classiquement, il est aussi possible d'utiliser un *algorithme probabiliste* simple pour répondre à la question, en évaluant la fonction f en k points $(x_1, \ldots, x_n)$ choisis indépendamment et uniformément au hasard dans l'ensemble $\{0,1\}^n$. L'algorithme est alors le suivant : si l'évaluation de f donne la même valeur pour les k points, déclarer que celle-ci est constante ; sinon, déclarer que celle-ci est balancée. Dans le second cas, la probabilité de faire une erreur est nulle, mais dans le premier, cette probabilité vaut $1/2^{k-1}$ si f est une fonction balancée. Avec une valeur de k fixée, mais suffisamment grande, cette probabilité d'erreur est tout à fait acceptable. Et donc pas besoin ici d'un nombre d'évaluations exponentiel en n.

Circuit de Deutsch-Josza pour $n = 2$ (pour alléger un peu les notations...)



Comme précédemment, analysons les états successifs des trois qubits dans ce circuit.

- L'état initial vaut $|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = |0,0,0\rangle$.

- Après le passage par les portes H (et la porte X pour le 3e qubit), l'état vaut :

$$|\psi_1\rangle = H|0\rangle \otimes H|0\rangle \otimes HX|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes H|1\rangle$$
$$= \frac{1}{2}(|0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle) \otimes |-\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} |x,y\rangle \otimes |-\rangle$$

- Pour calculer l'état $|\psi_2\rangle$, observons que, similairement à la semaine dernière :

$$U_f(|x,y\rangle \otimes |-\rangle) = (-1)^{f(x,y)}|x,y\rangle \otimes |-\rangle$$

En effet, nous avons :

$$U_f(|x,y\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}}(U_f|x,y,0\rangle - U_f|x,y,1\rangle) = \frac{1}{\sqrt{2}}\left(|x,y,f(x,y)\rangle - \left|x,y,\overline{f(x,y)}\right\rangle\right)$$

Si $f(x,y) = 0$, cette expression est égale à $\frac{1}{\sqrt{2}}(|x,y,0\rangle - |x,y,1\rangle) = |x,y\rangle \otimes |-\rangle$

Si $f(x,y) = 1$, cette expression est égale à $\frac{1}{\sqrt{2}}(|x,y,1\rangle - |x,y,0\rangle) = -|x,y\rangle \otimes |-\rangle$

Donc en résumé, nous trouvons bien $U_f(|x,y\rangle \otimes |-\rangle) = (-1)^{f(x,y)}|x,y\rangle \otimes |-\rangle$, et par linéarité :

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} (-1)^{f(x,y)}|x,y\rangle \otimes |-\rangle$$

- Finalement, l'état $|\psi_3\rangle$ est donné par

$$|\psi_3\rangle = (H \otimes H \otimes I)|\psi_2\rangle = \frac{1}{2}\sum_{x,y\in\{0,1\}} (-1)^{f(x,y)} H|x\rangle \otimes H|y\rangle \otimes |-\rangle$$
$$= \frac{1}{2}\sum_{x,y\in\{0,1\}} (-1)^{f(x,y)} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y|1\rangle) \otimes |-\rangle$$
$$= \frac{1}{4}\sum_{x,y\in\{0,1\}} (-1)^{f(x,y)}\Big(|0,0\rangle + (-1)^y|0,1\rangle + (-1)^x|1,0\rangle + (-1)^{x+y}|1,1\rangle\Big) \otimes |-\rangle$$

Même s'il peut paraître a priori difficile (voire fatigant) de déchiffrer, à partir de l'expression de la page précédente, les probabilités de sortie des différents états après la mesure, concentrons-nous tout d'abord sur la probabilité de sortie de l'état $|0,0\rangle$. Celle-ci est donnée par

$$\text{prob}(0,0) = \left(\frac{1}{4} \sum_{x,y \in \{0,1\}} (-1)^{f(x,y)} \right)^2$$

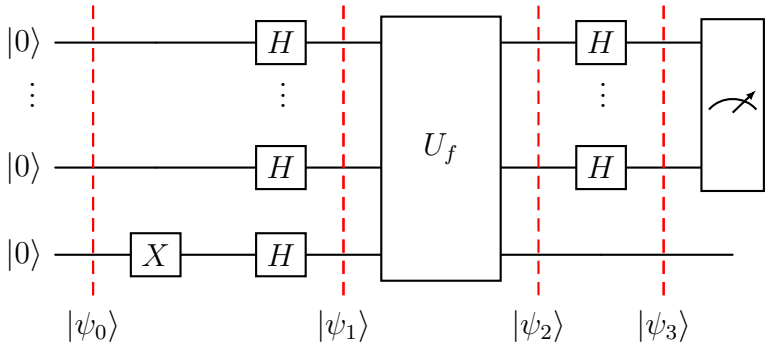
Observez que si f est une fonction constante, alors $\text{prob}(0,0) = \left(\frac{1}{4}\, 4\, (-1)^{f(0,0)}\right)^2 = 1$.

Tandis que si f est une fonction balancée, alors $\text{prob}(0,0) = \left(\frac{1}{4} \sum_{x,y \in \{0,1\}} (-1)^{f(x,y)}\right)^2 = 0$, car la fonction f vaut 1 pour la moitié des points (x,y) et 0 pour l'autre moitié ; les -1 et les $+1$ se compensent donc exactement dans la somme.

Que déduire de là ? que f est constante si et seulement si l'état $|0,0\rangle$ est observé après la mesure. Si n'importe quel autre état est observé après la mesure, alors f est balancée.

Et tout ceci avec un seul appel à l'oracle U_f.

Généralisation à n qubits (donnée ici par souci d'exhaustivité...)



Voici comment s'écrivent les états successifs des $n+1$ qubits dans ce cas plus général :

- $|\psi_0\rangle = |0,\ldots,0,0\rangle$

- $|\psi_1\rangle = H|0\rangle \otimes \cdots \otimes H|0\rangle \otimes HX|0\rangle = \dfrac{1}{2^{n/2}} \displaystyle\sum_{x_1,\ldots,x_n \in \{0,1\}} |x_1,\ldots,x_n\rangle \otimes |-\rangle$

- De la même façon que précédemment, $U_f\,(|x_1,\ldots,x_n\rangle \otimes |-\rangle) = (-1)^{f(x_1,\ldots,x_n)}\,|x_1,\ldots,x_n\rangle \otimes |-\rangle$, donc

$$|\psi_2\rangle = U_f\,|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{f(x_1,\ldots,x_n)}\,|x_1,\ldots,x_n\rangle \otimes |-\rangle$$

- Finalement, $|\psi_3\rangle = (H^{\otimes n} \otimes I)\,|\psi_2\rangle = \dfrac{1}{2^{n/2}} \displaystyle\sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{f(x_1,\ldots,x_n)} H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle \otimes |-\rangle$

En notant que pour $1 \leq i \leq n$, $H|x_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_i}|1\rangle) = \frac{1}{\sqrt{2}} \sum_{y_i \in \{0,1\}} (-1)^{x_i y_i} |y_i\rangle$, nous obtenons :

$$H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle = \frac{1}{2^{n/2}} \sum_{y_1,\ldots,y_n \in \{0,1\}} (-1)^{x_1 y_1 + \cdots + x_n y_n} |y_1, \ldots, y_n\rangle$$

ce qui donne l'expression suivante pour $|\psi_3\rangle$ (après quelques permutations/regroupements de termes):

$$|\psi_3\rangle = \sum_{y_1,\ldots,y_n \in \{0,1\}} \left(\frac{1}{2^n} \sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{f(x_1,\ldots,x_n) + x_1 y_1 + \cdots + x_n y_n} \right) |y_1, \ldots, y_n\rangle \otimes |-\rangle$$

A nouveau, calculer les probabilités de sortie des différents état après la mesure peut sembler cauchemardesque, mais en se restreignant à l'état $|0, \ldots, 0\rangle$, nous trouvons que la probabilité de sortie de cet état est donnée par

$$\left(\frac{1}{2^n} \sum_{x_1,\ldots,x_n \in \{0,1\}} (-1)^{f(x_1,\ldots,x_n)} \right)^2$$

qui vaut 1 si f est constante et 0 si f est balancée, comme précédemment.