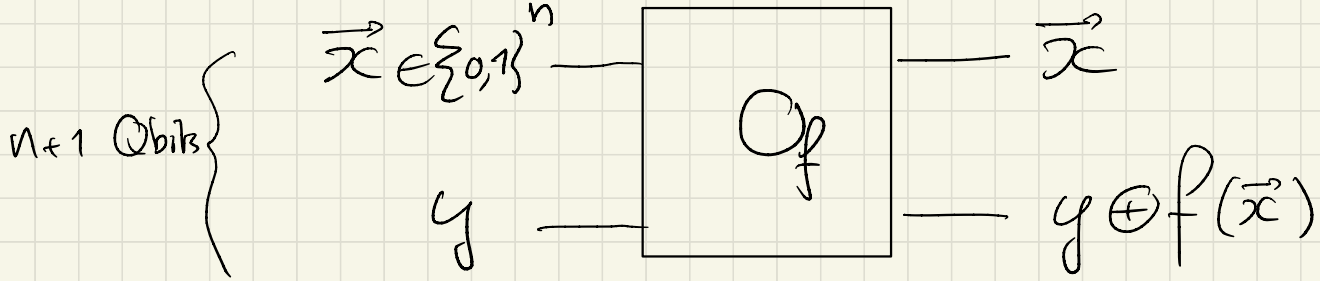
Généralisation : 2 Qbits $\longrightarrow$ n+1 Qbits

Le but ici est de répondre à des questions concernant une fonction $f : \{0,1\}^n \longrightarrow \{0,1\}$ en utilisant un nombre minimum de fois la porte O_f :



Etat initial : $|\psi_0\rangle = \underbrace{\left(\frac{1}{2^{n/2}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle\right)}_{\text{superposition de } 2^n \text{ etats !}} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

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

$$= |\vec{x}\rangle \otimes (-1)^{f(\vec{x})} \cdot \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad \text{magic!}$$

$$= (-1)^{f(\vec{x})} |\vec{x}\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Donc $|\psi_1\rangle = O_f |\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{\vec{x}} |\vec{x}\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

laissons tomber le $(n+1)^e$ bit (qui a bien servi)

Nous nous retrouvons maintenant, après une seule évaluation de la fonction f, avec un système dans l'état :

$$|\tilde{\varphi}_1\rangle = \frac{1}{2^{n/2}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})} |\vec{x}\rangle$$

A partir de là, on peut faire plein de choses intéressantes ...

1. Algorithme de Deutsch-Josza

Supposons qu'on nous dise que la fonction f est :

- soit constante : $f(\vec{x}) = f(\vec{y}) \quad \forall \vec{x}, \vec{y} \in \{0,1\}^n$
- soit balancée, i.e. :

$$\begin{cases} f(\vec{x}) = 0 & \text{pour la moitié des } \vec{x} \in \{0,1\}^n \\ f(\vec{x}) = 1 & \text{pour l'autre moitié des } \vec{x} \end{cases}$$

Classiquement, pour évaluer si f est constante ou balancée, on devra évaluer la fonction f en $2^{n/2}+1$ valeurs de $\vec{x}$, dans le pire des cas (i.e. si on est très malchanceux).

(NB : En pratique, l'algorithme probabiliste qui essaye des valeurs de $\vec{x}$ au hasard trouve la réponse en temps constant, à 99%.)

Avec un circuit quantique, la réponse est obtenue après une seule évaluation de f :

On reprend notre état $|\tilde{\varphi}_1\rangle = \frac{1}{2^{n/2}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})} |\vec{x}\rangle$ et on fait passer chacun des n Q bits à travers une porte de Hadamard H :

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\Rightarrow H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{x \cdot y} |y\rangle \quad \text{pour } x \in \{0,1\}$$

$$\Rightarrow H^{\otimes n}|\vec{x}\rangle = \underbrace{(H \otimes \dots \otimes H)}_{n \text{ fois}}|\vec{x}\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{\vec{y} \in \{0,1\}^n} (-1)^{\vec{x}\cdot\vec{y}} |\vec{y}\rangle$$

$$\Rightarrow |\tilde{\varphi}_2\rangle = H^{\otimes n}|\tilde{\varphi}_1\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})} \cdot \frac{1}{2^{n/2}} \sum_{\vec{y} \in \{0,1\}^n} (-1)^{\vec{x}\cdot\vec{y}} \cdot |\vec{y}\rangle$$

$$= \sum_{\vec{y} \in \{0,1\}^n} \underbrace{\left(\frac{1}{2^n} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x}) + \vec{x}\cdot\vec{y}} \right)}_{= A(\vec{y})} \cdot |\vec{y}\rangle$$

$|\tilde{\psi}_2\rangle$ est donc une superposition d'états $|\vec{y}\rangle$ avec $\vec{y} \in \{0,1\}^n$ et amplitude correspondante $A(\vec{y})$ pour chaque état.

<u>Observation</u> : $A(\vec{0}) = \frac{1}{2^n} \sum_{\vec{x} \in \{0,1\}^n} (-1)^{f(\vec{x})}$

Donc
- Si $f = cte$, $|A(\vec{0})|^2 = 1$ ($f(\vec{x}) = 0$ pour tout $\vec{x}$ ou $f(\vec{x}) = 1$ pour tout $\vec{x}$)
- Si f est balancée, $|A(\vec{0})|^2 = 0$ (les + et les − se compensent)

En conclusion :

(↔ 1er @ bit pour le pb de Deutsch)

- Si on mesure l'état $|\tilde{\varphi}_2\rangle$ et qu'on obtient l'état $|\vec{0}\rangle$, on est sûr alors que la fonction est cte.
- Si on mesure l'état $|\tilde{\varphi}_2\rangle$ et qu'on obtient un état différent de $|\vec{0}\rangle$ (n'importe lequel) on est sûr alors que la fonction est balancée.

(et tout ceci en une seule évaluation de la fonction f)

2. Algorithme de Bernstein-Vazirani

Supposons maintenant que la fonction f soit de la forme

$$f(\vec{x}) = \vec{s} \cdot \vec{x} = s_1 x_1 + \dots + s_n x_n$$

avec $\vec{s} \in \{0,1\}^n$

Classiquement, pour découvrir le vecteur $\vec{s}$ il faut évaluer la fonction f en n positions $\vec{x}$:

$\vec{x_1} = (1000\dots)$, $\vec{x_2} = (0100\dots)$ etc.

Avec un algorithme quantique, ceci est à nouveau possible en une seule évaluation:

Reprenons le circuit précédent:

$$|\psi_2\rangle = \sum_{\vec{y}\in\{0,1\}^n} \underbrace{\left(\frac{1}{2^n} \sum_{\vec{x}\in\{0,1\}^n} (-1)^{f(\vec{x})+\vec{x}\cdot\vec{y}} \right)}_{=A(\vec{y})} |\vec{y}\rangle$$

$$\text{Or } A(\vec{y}) = \frac{1}{2^n} \sum_{\vec{x}\in\{0,1\}^n} (-1)^{(\vec{s}+\vec{y})\cdot\vec{x}} = \begin{cases} 1 & \text{si } \vec{y}=\vec{s} \\ 0 & \text{si } \vec{y}\neq\vec{s} \end{cases}$$

Donc une observation suffit pour trouver le vecteur $\vec{s}$.