Algorithme de Deutsch-Jozsa

1 Problème à résoudre

Soit une fonction f définie par

$$f : \{0,1\}^n \to \{0,1\}$$

$$(x_0, x_1, \ldots, x_n) \mapsto y = f(x_0, x_1, \ldots, x_n),$$

Définition 1. *Une fonction est dite équilibrée si f retourne 0 pour la moitié de ses entrées.*

Définition 2. *Une fonction est dite constante si elle retourne 0 pour toutes ses entrées.*

Problème 1. *Etant donnée une fonction f qui est soit équilibrée, soit constante. Le problème de Deutsch-Jozsa est de déterminer si f est constante ou non.*

1.1 Solution classique

Dans le cas classique, il faut effectuer au pire $2^{n-1} + 1$ évaluations pour déterminer si f est constante ou équilibrée. Tout d'abord, dès que deux évaluations sont différentes, f est nécessairement équilibrée. De plus, si après avoir évalué 2^{n-1} entrées et obtenu la même valeur, une évaluation supplémentaire nous permet de connaitre dans quelle catégorie f se trouve.

1.2 Solution quantique

Dans le cas quantique, ce problème se résout en une seule évaluation quantique de f.

1.2.1 Initialisation

On commence avec : $|u_0\rangle = |0\rangle^{\bigotimes n}|1\rangle$: n-qubits à $|0\rangle$ et 1-qubit à $|1\rangle$

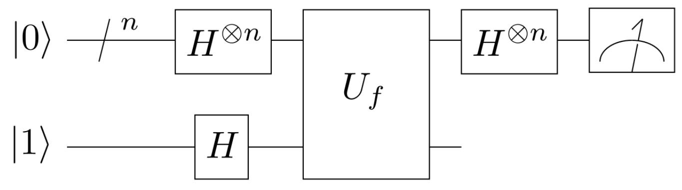

Figure 1: Schéma de l'algorithme

1.2.2 Etape 1

On applique une porte de Hadamard à $|u_0\rangle$ pour avoir un état équiprobable:
$|u_1\rangle = H|u_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$

1.2.3 Etape 2

On applique l'oracle quantique suivant à $|u_1\rangle$: $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$
Prenons le cas à 1 qubit:

$$f(x) = 0 : |x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|0\rangle - |1\rangle)$$

$$f(x) = 1 : |x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|1\rangle - |0\rangle)$$

$$f(x) quelconque : |x\rangle(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

En généralisant:
$|u_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$
On peut ignorer le dernier qubit $(|0\rangle - |1\rangle)$ comme il est constant. Finalement, on en déduit :
$|u_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle$

1.2.4 Etape 3

On réapplique une porte Hadamard à chaque qubit sortant, ce qui donne:
$|u_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x.y}|y\rangle$
$|u_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)}(-1)^{x.y}|y\rangle$
La probabilité de mesurer $|0\rangle^{\bigotimes n}$ est : $|\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|$

Si on obtient 0, alors $f(x)$ est constante. Si on obtient 1, alors $f(x)$ est équilibrée.