

Algorithme de Deutsch-Jozsa

1 Problème à résoudre

Soit une fonction f définie par

$$f : \{0, 1\}^n \rightarrow \{0, 1\}$$
$$(x_0, x_1, \dots, x_n) \mapsto y = f(x_0, x_1, \dots, x_n),$$

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 connaître 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 : $|u_0\rangle = |0\rangle^{\otimes n} |1\rangle$: n -qubits à $|0\rangle$ et 1-qubit à $|1\rangle$

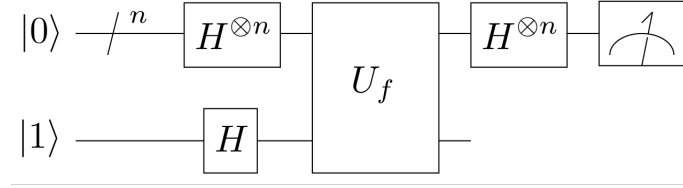


FIGURE 1 – Schéma de l'algorithme

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 :

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

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

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

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 :

$$|u_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

$$|u_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle$$

La probabilité de mesurer $|0\rangle^{\otimes n}$ 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.

1.3 Example

Prenons une fonction f comme définie précédemment, sans savoir si elle est constante ou équilibrée.

1.3.1 Etape 1

On commence avec $|u_0\rangle = |001\rangle$. La première étape est l'application de la porte d'hadamard à $|u_0\rangle$:

$$\begin{aligned} |u_1\rangle &= H|u_0\rangle = H|0\rangle \otimes H|0\rangle \otimes H|1\rangle \\ |u_1\rangle &= \frac{1}{2\sqrt{2}}\{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)\} \\ |u_1\rangle &= \frac{1}{2\sqrt{2}}\{|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle\} \\ \text{On peut factoriser le tout par } (|0\rangle - |1\rangle) : \\ |u_1\rangle &= \frac{1}{2\sqrt{2}}\{|00\rangle(|0\rangle - |1\rangle) + |01\rangle(|0\rangle - |1\rangle) + |10\rangle(|0\rangle - |1\rangle) + |11\rangle(|0\rangle - |1\rangle)\} \end{aligned}$$

1.3.2 Etape 2 : oracle quantique

On applique à $|u_1\rangle$ l'oracle quantique $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$:

$$\begin{aligned} |u_2\rangle &= \frac{1}{2\sqrt{2}}[\\ &|00\rangle(|0 \oplus f(00)\rangle - |1 \oplus f(00)\rangle) + \\ &|01\rangle(|0 \oplus f(01)\rangle - |1 \oplus f(01)\rangle) + \\ &|10\rangle(|0 \oplus f(10)\rangle - |1 \oplus f(10)\rangle) + \\ &|11\rangle(|0 \oplus f(11)\rangle - |1 \oplus f(11)\rangle)] \end{aligned}$$

On peut alors réécrire l'équation de la façon suivante :

$$\begin{aligned} |u_2\rangle &= \frac{1}{2\sqrt{2}}[\\ &(-1)^{f(00)}|00\rangle(|0\rangle - |1\rangle) + \\ &(-1)^{f(01)}|01\rangle(|0\rangle - |1\rangle) + \\ &(-1)^{f(10)}|10\rangle(|0\rangle - |1\rangle) + \\ &(-1)^{f(11)}|11\rangle(|0\rangle - |1\rangle)] \end{aligned}$$

Par la suite, on va appliquer une porte de Hadamard à $|u_2\rangle$. Le qubit $|0\rangle - |1\rangle$ donne $|1\rangle$ par la cette porte, il est donc constant par rapport à $|u_0\rangle$. On peut donc le retirer de l'équation, ce qui nous donne pour $|u_2\rangle$:

$$|u_2\rangle = \frac{1}{2\sqrt{2}}[(-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle]$$

1.3.3 Etape 3 : porte de Hadamard

On applique donc une porte de hadamard à $|u_2\rangle$:

$$|u_3\rangle = \frac{1}{2\sqrt{2}} H[(-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle]$$

Nous sommes sur une porte de hadamard pour 2 qubits, ce qui donne l'équation matricielle suivante pour l'état A de $|u_3\rangle$:

$$A = \frac{1}{4\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} (-1)^{f(00)} \\ (-1)^{f(01)} \\ (-1)^{f(10)} \\ (-1)^{f(11)} \end{bmatrix} = \frac{1}{4\sqrt{2}} \begin{bmatrix} (-1)^{f(00)} + (-1)^{f(01)} + (-1)^{f(10)} + (-1)^{f(11)} \\ (-1)^{f(00)} - (-1)^{f(01)} + (-1)^{f(10)} - (-1)^{f(11)} \\ (-1)^{f(00)} + (-1)^{f(01)} - (-1)^{f(10)} - (-1)^{f(11)} \\ (-1)^{f(00)} - (-1)^{f(01)} - (-1)^{f(10)} + (-1)^{f(11)} \end{bmatrix}$$

Si f est constante, alors $(-1)^{f(00)} = (-1)^{f(01)} = (-1)^{f(10)} = (-1)^{f(11)} = 1$.

On a donc :

$$A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Et donc une probabilité de 1 de mesurer l'état $|00\rangle$.

En revanche, si f est équilibrée, la moitié des valeurs vont valoir $(-1)^0 = 1$ et l'autre moitié $(-1)^1 = -1$. La première ligne du vecteur A donne donc systématiquement 0, on ne mesure donc jamais l'état $|00\rangle$.