Algorithme de Deutsch-Jozsa

1 Problème à résoudre

Soit une fonction f booléenne définie par

$$\begin{array}{rccl} f: & \{0,1\}^n & \to & \{0,1\} \\ & (x_0, x_1, \ldots, x_n) & \mapsto & y = f(x_0, x_1, \ldots, x_n), \end{array}$$

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

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

Remarque 1. *Avec n un entier et comme les fonctions booléennes sont à valeur dans $\{0,1\}$, il n'existe que deux fonctions constantes f_0 et f_1.*

Exemple 1. *Soit f la fonction booléenne $f : \{0,1\}^2 \to \{0,1\}$ définie par la table de vérité suivante :*

(x_1, x_2)	$f(x_1, x_2)$
$(0,0)$	0
$(0,1)$	1
$(1,0)$	1
$(1,1)$	0

Cette fonction est équilibrée. On notera qu'elle correspond au classique "ou exclusif". Cette fonction pourrait être représentée par le vecteur de ces valeurs : $(0,1,1,0)$. Elle peut aussi être codée en listant les emplacements où elle est vraie, ici $\{1,2\}$.

Remarque 2. *Dénombrer les fonctions équilibrées revient à dénombrer les façons de placer le symbole le symbole 1 dans la moitié des cases d'un vecteur de taille 2^n. Avec les emplacements, cela revient à dénombrer l'ensemble de*

sous-ensembles de $\{0, \ldots, 2^n - 1\}$ *qui ont pour cardinal* $2^n/2$. *Finalement, il a donc* $\binom{2^n}{2^{n-1}}$ *fonctions équilibrées. Ce qui fait*

$$\binom{2^n}{2^{n-1}} = \frac{(2^n)!}{(2^{n-1})!(2^n - 2^{n-1})!} = \frac{(2^n)!}{((2^{n-1})!)^2}.$$

On notera que la proportion des fonctions équilibrées sur l'ensemble des 2^{2^n} *fonctions booléennes de* n *variables diminue très rapidement avec* n.

Problème 1 (Deutsch-Jozsa)**.** *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.

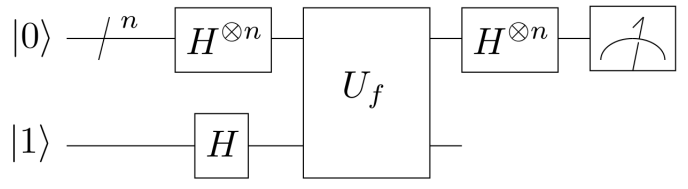

FIGURE 1 – Schéma de l'algorithme

1.2.1 Initialisation

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

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 $|u_1\rangle$:

$$o : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle.$$

Posons x, on est alors dans l'une des deux situations disjointes suivantes :
— $f(x) = 0$,
— $f(x) = 1$.
Analysons chacune de ces situations, tout d'abord si $f(x) = 0$ alors

$$o : |x\rangle(|0\rangle - |1\rangle) \mapsto |x\rangle(|0\rangle - |1\rangle)$$

Autrement dit $|x\rangle(|0\rangle - |1\rangle$ est un point fixe de o.

Dans l'autre situation, on a $f(x) = 1$ et on en déduit

$$o : |x\rangle(|0\rangle - |1\rangle) \mapsto |x\rangle(|1\rangle - |0\rangle)$$

Autrement dit, dans ce cas, le vecteur $|x\rangle(|0\rangle - |1\rangle)$ est envoyé sur son opposé via o.

Finalement, les deux cas précédents peuvent être résumé sous la forme suivante

$$o : |x\rangle(|0\rangle - |1\rangle) \mapsto (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Par linéarité, on en déduit :

$$|u_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \tag{1}$$

On peut ignorer le dernier qubit $(|0\rangle - |1\rangle)$ comme il est constant. Finalement, on en déduit :

$$|u_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle \tag{2}$$

1.2.4 Etape 3

Maintenant qu'on a appliqué notre oracle, on est toujours dans un état "probabiliste", et en mesurant nous n'obtiendrons pas une réponse exacte à notre problème. L'objectif est donc maintenant de ramener les solutions sur un état déterminé pour obtenir la réponse systématique. En appliquant la porte de Hadamard, on va pouvoir forcer un état à apparaître pour un type de fonction f, et le forcer à disparaître dans l'autre cas, ce qui nous permet d'avoir une réponse systématique sur le type de la fonction : est-elle équilibrée ou bien constante ?

On réapplique une porte Hadamard à chaque qubit sortant, ce qui donne :

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

Par linéarité, on a :

$$|u_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{x.y} |y\rangle \tag{3}$$

La probabilité $|p|$ de mesurer $|0\rangle^{\bigotimes n}$ est donc :

$$|\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}| \tag{4}$$

avec $p = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}$.

Si on a une fonction $f(x)$ constante, alors chaque élément de la somme retourne la même valeur (1 ou -1 suivant que $f(x)$ retourne 0 ou 1), la somme va donc valoir $\pm 2^n$. Dans le cas où la fonction est équilibrée, on va avoir autant de 1 que de -1, la somme est donc nulle.

On a donc les valeurs suivantes dépendant du type de $f(x)$:

1. Si $f(x)$ est constante : $p = \pm\frac{1}{2^n} \times 2^n = \pm 1$,
2. Si $f(x)$ est équilibrée : $p = \pm\frac{1}{2^n} \times 0 = 0$.

Dans le cas constant, on ne peut donc que mesurer $|0\rangle^{\bigotimes n}$ puisqu'il a une probabilité de 1 d'apparaître. Dans le cas équilibré, on ne mesure jamais $|0\rangle^{\bigotimes n}$ puisque sa probabilité est nulle.

On en conclut que, lorsqu'on effectue une mesure, si on tombe sur $|0\rangle^{\bigotimes n}$ alors la fonction est constante, sinon elle est équilibrée.

1.3 Exemple

Prenons une fonction f comme définie précédemment avec $n = 2$, 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 $|u_0\rangle$:

$$|u_1\rangle = H|u_0\rangle = H|0\rangle \otimes H|0\rangle \otimes H|1\rangle \tag{5}$$

$$= \frac{1}{2\sqrt{2}} \left((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \right) \tag{6}$$

$$= \frac{1}{2\sqrt{2}} \{|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle\} \tag{7}$$

$$= \frac{1}{2\sqrt{2}} \{|00\rangle(|0\rangle - |1\rangle) + |01\rangle(|0\rangle - |1\rangle) + |10\rangle(|0\rangle - |1\rangle) + |11\rangle(|0\rangle - |1\rangle)\} \tag{8}$$

1.3.2 Etape 2 : oracle quantique

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

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

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 $|u_2\rangle$:

$$|u_2\rangle = \frac{1}{2\sqrt{2}} \left((-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle \right) \tag{9}$$

Matriciellement, on peut donc écrire

$$|u_2\rangle = \begin{pmatrix} (-1)^{f(00)} & 0 & 0 & 0 \\ 0 & (-1)^{f(01)} & 0 & 0 \\ 0 & 0 & (-1)^{f(10)} & 0 \\ 0 & 0 & 0 & (-1)^{f(11)} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \tag{10}$$

1.3.3 Etape 3 : porte de Hadamard

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

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

Nous sommes sur une porte de hadamard pour 2 qubits, ce qui donne la relation matricielle suivante pour $|u_3\rangle$:

$$|u_3\rangle = \frac{1}{4\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} (-1)^{f(00)} \\ (-1)^{f(01)} \\ (-1)^{f(10)} \\ (-1)^{f(11)} \end{bmatrix}, \tag{12}$$

$$= \frac{1}{4\sqrt{2}} \begin{bmatrix} (-1)^{f(00)} + (-1)^{f(01)} + (-1)^{f(10)} + (-1)^{f(11)} \\ (-1)^{f(00)} - (-1)^{f(01)} + (-1)^{f(10)} - (-1)^{f(11)} \\ (-1)^{f(00)} + (-1)^{f(01)} - (-1)^{f(10)} - (-1)^{f(11)} \\ (-1)^{f(00)} - (-1)^{f(01)} - (-1)^{f(10)} + (-1)^{f(11)} \end{bmatrix}. \tag{13}$$

Si f est constante , alors $(-1)^{f(00)} = (-1)^{f(01)} = (-1)^{f(10)} = (-1)^{f(11)}$. En fonction du fait que $f = 0$ ou bien $f = 1$:

$$|u_3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ ou bien } |u_3\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{14}$$

On a 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 $|u_3\rangle$ donne donc systématiquement 0, on ne mesure donc jamais l'état $|00\rangle$.