Algorithme de Deutsch–Jozsa

Vidéo ■ partie 10. Algorithme de Deutsch-Jozsa

Nous expliquons et prouvons l'algorithme de Deutsch–Jozsa dans le cas général. C'est notre premier algorithme quantique qui supplante les algorithmes classiques et c'est aussi l'occasion d'introduire plusieurs notions utiles pour la suite.

1. Algorithme

1.1. Problème

Le problème à résoudre est la généralisation du problème rencontré dans le chapitre introductif « Un premier algorithme quantique ».

Terminologie. Soit une fonction $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$, que l'on peut aussi voir comme une fonction $f : \{0,1\}^n \to \{0,1\}$. Il y a $2^{(2^n)}$ fonctions différentes possibles mais nous n'allons considérer que deux types de fonctions.

- f est ***constante*** si pour tout $(x_1,\dots,x_n)$ on a $f(x_1,\dots,x_n)=0$ ou bien si pour tout $(x_1,\dots,x_n)$ on a $f(x_1,\dots,x_n)=1$. Il existe donc deux fonctions constantes.
- f est ***équilibrée*** s'il y a autant de n-uplets $(x_1,\dots,x_n)$ tels que $f(x_1,\dots,x_n)=0$ que de n-uplets $(x_1,\dots,x_n)$ tels que $f(x_1,\dots,x_n)=1$, autrement dit

$$\begin{aligned}&\text{Card}\left\{(x_1,\dots,x_n)\in(\mathbb{Z}/2\mathbb{Z})^n \mid f(x_1,\dots,x_n)=0\right\}\\ &\qquad = \text{Card}\left\{(x_1,\dots,x_n)\in(\mathbb{Z}/2\mathbb{Z})^n \mid f(x_1,\dots,x_n)=1\right\}.\end{aligned}$$

  Il y a en tout $\binom{2^n}{2^{n-1}} = \frac{2^n!}{(2^{n-1}!)^2}$ telles fonctions.

Pour $n>1$ il existe beaucoup de fonctions qui ne sont ni constantes, ni équilibrées, par exemple une fonction qui prend une seule fois la valeur 1 et 0 ailleurs.

Problème. On nous donne une fonction $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ en nous certifiant qu'elle est soit constante, soit équilibrée. C'est à vous de déterminer dans quelle catégorie elle se situe : constante ou équilibrée.

1.2. Solution classique

Pour ce problème, la complexité des algorithmes se mesure par le nombre d'évaluations $f(x_1,\dots,x_n)$ effectuées. Avec un ordinateur classique, la complexité du meilleur algorithme est exponentielle, d'ordre $O(2^n)$. Notons qu'il y a en tout $2^n = \text{Card}((\mathbb{Z}/2\mathbb{Z})^n)$ éléments dans l'ensemble de départ. Voici un algorithme classique dont la complexité est $2^{n-1}+1$.

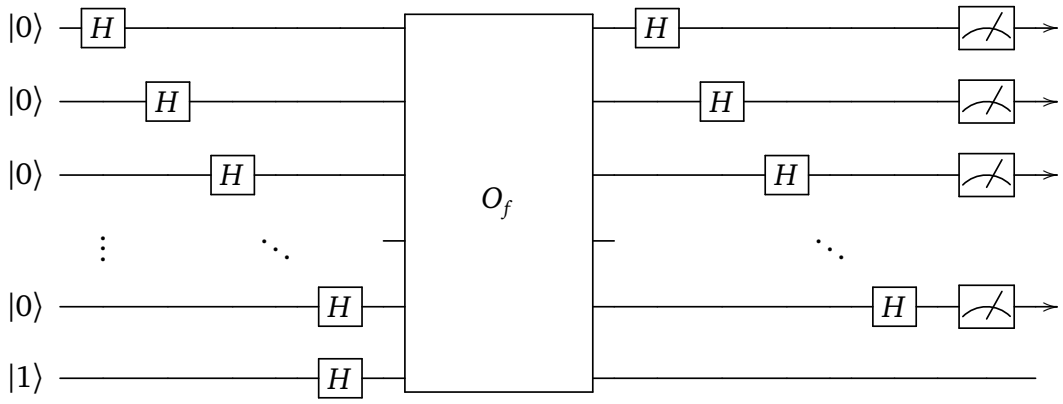
Algorithme.

- On évalue f sur $2^{n-1}+1$ termes.
- Si toutes ces valeurs sont égales alors f est constante, sinon elle est équilibrée.

Plus précisément, aucun algorithme classique ne peut faire moins que $\frac{2^n}{2}$ évaluations. Bien sûr pour certaines fonctions f on pourrait obtenir une réponse plus rapide (par exemple dès que l'on obtient deux valeurs différentes, la fonction doit être équilibrée), mais dans le pire des cas il faut évaluer f sur plus de la moitié des éléments pour pouvoir conclure. En effet, si par exemple f s'annule sur la moitié des éléments, on ne peut pas déjà savoir si elle est constante ou équilibrée car les deux conclusions sont encore possibles.

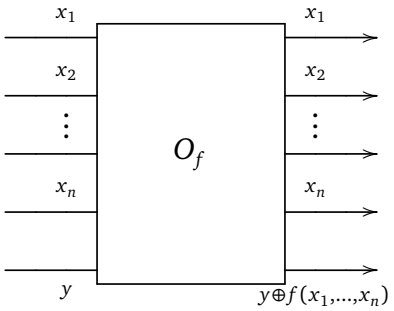
1.3. Circuit quantique

Voici le circuit qui fournit l'algorithme quantique répondant au problème.



Les n premières lignes du circuit sont initialisées par $|0\rangle$, suivi de la transformation de Hadamard. La dernière ligne est initialisée par $|1\rangle$, suivi d'une porte de Hadamard. Ensuite on applique l'oracle associé à f. Enfin, on applique de nouveau une transformation de Hadamard sur les n premières lignes, suivi d'une mesure uniquement sur les n premières lignes.
Le circuit n'est exécuté qu'une seule fois, autrement dit l'algorithme quantique est de complexité 1 car la fonction associée à l'oracle O_f n'est évaluée qu'une seule fois.

L'algorithme consiste simplement à exécuter le circuit.
Algorithme. Si la mesure des n premiers qubits de sortie est $0.0\ldots0$ alors la fonction est constante, sinon la fonction est équilibrée.
Pour les exemples où $n = 1$ ou $n = 2$, nous renvoyons au chapitre « Un premier algorithme quantique ». La complexité de l'algorithme quantique est donc $O(1)$. On a vu que l'algorithme classique est de complexité exponentielle. En effet $O(2^{n-1}) = O(2^n)$ et $2^n = e^{n\ln 2}$. L'algorithme quantique est donc une amélioration exponentielle de l'algorithme classique ! Bien sûr le problème résolu ici est artificiel et assez peu intéressant mais nous avons maintenant la preuve que l'informatique quantique peut aller plus vite que l'informatique classique.
On rappelle que l'oracle associé à la fonction f agit ainsi : sur les n premières lignes $x_i \mapsto x_i$, sur la dernière ligne $y \mapsto y \oplus f(x_1, \ldots, x_n)$.



2. Notation entière des qubits

2.1. Notation

La notation $|0.0\dots0\rangle$, $|0.0\dots1\rangle$,…,$|1.1\dots1\rangle$ pour les n-qubits de la base canonique n'est pas pratique pour les calculs généraux et les preuves. En particulier comment noter un n-qubit quelconque de cette base ? Nous allons introduire l'écriture d'un n-qubit de base par un seul entier : c'est tout simplement l'opération inverse de l'écriture binaire.
On fixe un entier $n \geqslant 1$. Soit $0 \leqslant k \leqslant 2^n - 1$. Notons $\underline{k}$ l'écriture binaire de l'entier k sur n bits. L'*écriture entière* $\left|\underline{k}\right\rangle$ désigne le n-qubit de la base canonique associé à l'écriture binaire de k.

$$\begin{aligned}
\left|\underline{0}\right\rangle &= |0.0\dots0.0.0\rangle \\
\left|\underline{1}\right\rangle &= |0.0\dots0.0.1\rangle \\
\left|\underline{2}\right\rangle &= |0.0\dots0.1.0\rangle \\
\left|\underline{3}\right\rangle &= |0.0\dots0.1.1\rangle \\
&\vdots \\
\left|\underline{2^n-2}\right\rangle &= |1.1\dots1.1.0\rangle \\
\left|\underline{2^n-1}\right\rangle &= |1.1\dots1.1.1\rangle
\end{aligned}$$

On peut ainsi écrire facilement certains énoncés. Par exemple une fonction $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ est constante si $f(\underline{k}) = 0$ pour tout k variant de 0 à $2^n - 1$ ou si $f(\underline{k}) = 1$ pour tout k variant de 0 à $2^n - 1$.

2.2. Exemples

Pour $n = 1$, il y a seulement deux qubits de base et on a $\left|\underline{0}\right\rangle = |0\rangle$ et $\left|\underline{1}\right\rangle = |1\rangle$.

Exemple.
Pour $n = 2$.

$$\begin{aligned}
\left|\underline{0}\right\rangle &= |0.0\rangle \\
\left|\underline{1}\right\rangle &= |0.1\rangle \\
\left|\underline{2}\right\rangle &= |1.0\rangle \\
\left|\underline{3}\right\rangle &= |1.1\rangle
\end{aligned}$$

Exemple.
Pour $n = 3$.

$$\begin{aligned}
\left|\underline{0}\right\rangle &= |0.0.0\rangle & \qquad \left|\underline{4}\right\rangle &= |1.0.0\rangle \\
\left|\underline{1}\right\rangle &= |0.0.1\rangle & \qquad \left|\underline{5}\right\rangle &= |1.0.1\rangle \\
\left|\underline{2}\right\rangle &= |0.1.0\rangle & \qquad \left|\underline{6}\right\rangle &= |1.1.0\rangle \\
\left|\underline{3}\right\rangle &= |0.1.1\rangle & \qquad \left|\underline{7}\right\rangle &= |1.1.1\rangle
\end{aligned}$$

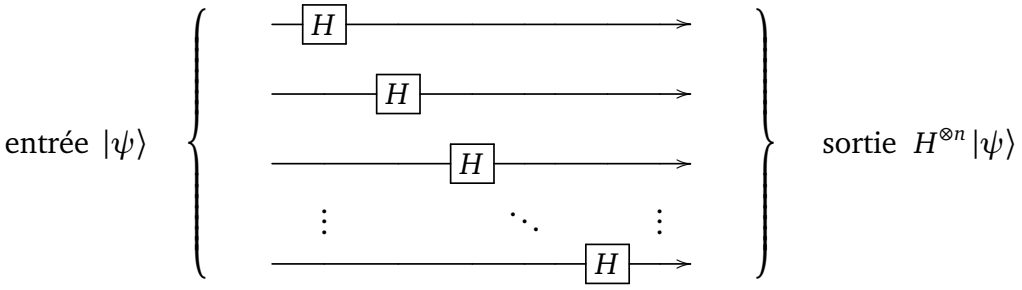
3. Transformation de Hadamard

3.1. Définition

On rappelle que la porte de Hadamard est définie pour les 1-qubits par la formule :

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{et} \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

La ***transformation de Hadamard*** d'un n-qubit $|\psi\rangle$ est l'application d'une porte de Hadamard sur chacun des 1-qubits le constituant. On note cette transformation $H^{\otimes n}$.
Le circuit est simplement composé de n lignes, avec une porte de Hadamard par ligne (l'ordre de ces portes n'a pas d'importance).



Exemple.
Pour $n = 2$.

$$\begin{aligned}
|\underline{0}\rangle = |0.0\rangle &\xmapsto{H^{\otimes 2}} \tfrac{1}{2}(|0+1\rangle|0+1\rangle) = \tfrac{1}{2}(|0.0\rangle + |0.1\rangle + |1.0\rangle + |1.1\rangle) = \tfrac{1}{2}(|\underline{0}\rangle + |\underline{1}\rangle + |\underline{2}\rangle + |\underline{3}\rangle)\\
|\underline{1}\rangle = |0.1\rangle &\xmapsto{H^{\otimes 2}} \tfrac{1}{2}(|0+1\rangle|0-1\rangle) = \tfrac{1}{2}(|0.0\rangle - |0.1\rangle + |1.0\rangle - |1.1\rangle) = \tfrac{1}{2}(|\underline{0}\rangle - |\underline{1}\rangle + |\underline{2}\rangle - |\underline{3}\rangle)\\
|\underline{2}\rangle = |1.0\rangle &\xmapsto{H^{\otimes 2}} \tfrac{1}{2}(|0-1\rangle|0+1\rangle) = \tfrac{1}{2}(|0.0\rangle + |0.1\rangle - |1.0\rangle - |1.1\rangle) = \tfrac{1}{2}(|\underline{0}\rangle + |\underline{1}\rangle - |\underline{2}\rangle - |\underline{3}\rangle)\\
|\underline{3}\rangle = |1.1\rangle &\xmapsto{H^{\otimes 2}} \tfrac{1}{2}(|0-1\rangle|0-1\rangle) = \tfrac{1}{2}(|0.0\rangle - |0.1\rangle - |1.0\rangle + |1.1\rangle) = \tfrac{1}{2}(|\underline{0}\rangle - |\underline{1}\rangle - |\underline{2}\rangle + |\underline{3}\rangle)
\end{aligned}$$

3.2. Formule de la transformation de Hadamard

Quelle est la formule qui permet de calculer la transformation de Hadamard sur les qubits de base ?

Exemple.
Calculons $H^{\otimes n}|\underline{0}\rangle$ pour n quelconque. Comme $|\underline{0}\rangle = |0.0\ldots0\rangle$ alors $H^{\otimes n}|\underline{0}\rangle = \frac{1}{\sqrt{2^n}}|0+1\rangle \cdot |0+1\rangle\cdots|0+1\rangle$. En développant ce produit, on obtient toutes les combinaisons possibles de 0 et de 1 :

$$\boxed{H^{\otimes n}|\underline{0}\rangle = \frac{1}{\sqrt{2^n}}(|0\ldots0.0\rangle + |0\ldots0.1\rangle + |0\ldots1.0\rangle + \quad\cdots\quad + |1\ldots1.1\rangle)}$$

Autrement dit :

$$\boxed{H^{\otimes n}|\underline{0}\rangle = \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}|\underline{\ell}\rangle}$$

La formule générale est donnée par la proposition suivante.

Proposition 1.
Pour $0 \leqslant k \leqslant 2^n - 1$, *on a :*

$$\boxed{H^{\otimes n} \left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{\ell=0}^{2^n-1} (-1)^{\underline{k}\odot\underline{\ell}} \left|\underline{\ell}\right\rangle}$$

Notation. Pour l'écriture binaire $\underline{k} = k_1.k_2 \ldots k_n$ et l'écriture binaire $\underline{\ell} = \ell_1.\ell_2 \ldots \ell_n$ (avec $k_i, \ell_i \in \{0,1\}$) alors

$$\underline{k} \odot \underline{\ell} = k_1\ell_1 \oplus k_2\ell_2 \oplus \cdots \oplus k_n\ell_n \quad \in \{0,1\}.$$

C'est comme un produit scalaire modulo 2.
Par exemple si $\left|\underline{k}\right\rangle = |0.1.0.1.1\rangle$ et $\left|\underline{\ell}\right\rangle = |1.1.0.0.1\rangle$ alors

$$\underline{k} \odot \underline{\ell} = 0\cdot 1 \oplus 1\cdot 1 \oplus 0\cdot 0 \oplus 1\cdot 0 \oplus 1\cdot 1 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 0.$$

Démonstration. $H^{\otimes n} \left|\underline{k}\right\rangle$ est un produit de termes ayant la forme $|0+1\rangle$ ou $|0-1\rangle$. En développant ce produit on obtient une expression faisant intervenir tous les n-qubits de la base canonique, donc tous les $\left|\underline{\ell}\right\rangle$, avec $\ell = 0, \ldots, 2^n - 1$.
On ne change le signe qu'en présence d'un 1 (donc il faut $\ell_i = 1$) et du signe « $-$ » (donc $k_i = 1$). Une preuve détaillée se fait par récurrence. □

3.3. Exemple

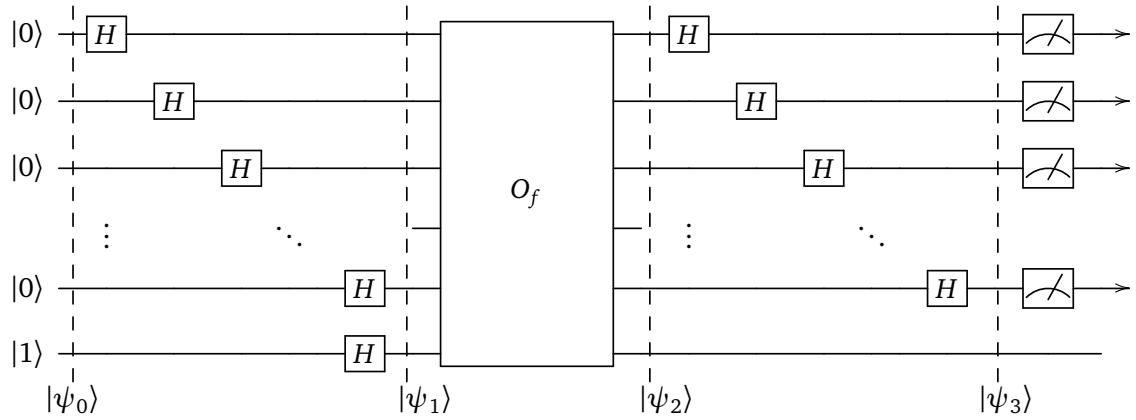
Exemple.
Soit $n = 3$ et $\left|\underline{k}\right\rangle = \left|\underline{5}\right\rangle = |1.0.1\rangle$, alors un calcul direct donne :

$$\begin{aligned} H^{\otimes 3} \left|\underline{5}\right\rangle &= H^{\otimes 3} |1.0.1\rangle \\ &= \tfrac{1}{2\sqrt{2}} |(0-1).(0+1).(0-1)\rangle \\ &= \tfrac{1}{2\sqrt{2}} \big(|0.0.0\rangle - |0.0.1\rangle + |0.1.0\rangle - |0.1.1\rangle - |1.0.0\rangle + |1.0.1\rangle - |1.1.0\rangle + |1.1.1\rangle \big) \end{aligned}$$

On retrouve bien la formule annoncée car avec $\underline{k} = \underline{5} = 1.0.1$ on a :

- pour $\ell = 0$: $\underline{\ell} = 0.0.0$, $\underline{k} \odot \underline{\ell} = 0$, donc terme $+|0.0.0\rangle$,
- pour $\ell = 1$: $\underline{\ell} = 0.0.1$, $\underline{k} \odot \underline{\ell} = 1$, donc terme $-|0.0.1\rangle$,
- pour $\ell = 2$: $\underline{\ell} = 0.1.0$, $\underline{k} \odot \underline{\ell} = 0$, donc terme $+|0.1.0\rangle$,
- pour $\ell = 3$: $\underline{\ell} = 0.1.1$, $\underline{k} \odot \underline{\ell} = 1$, donc terme $-|0.1.1\rangle$,
- pour $\ell = 4$: $\underline{\ell} = 1.0.0$, $\underline{k} \odot \underline{\ell} = 1$, donc terme $-|1.0.0\rangle$,
- pour $\ell = 5$: $\underline{\ell} = 1.0.1$, $\underline{k} \odot \underline{\ell} = 0$, donc terme $+|1.0.1\rangle$,
- pour $\ell = 6$: $\underline{\ell} = 1.1.0$, $\underline{k} \odot \underline{\ell} = 1$, donc terme $-|1.1.0\rangle$,
- pour $\ell = 7$: $\underline{\ell} = 1.1.1$, $\underline{k} \odot \underline{\ell} = 0$, donc terme $+|1.1.1\rangle$.

4. Preuve de l'algorithme de Deutsch–Jozsa



- Initialisation.

$$|\psi_0\rangle = |0\ldots0\rangle \cdot |1\rangle = \left|\underline{0}\right\rangle \cdot |1\rangle\,.$$

On mélange les deux écritures : la notation entière qui regroupe les n premiers qubits et la notation classique pour le dernier qubit.

- Transformation de Hadamard.

$$\begin{aligned}|\psi_1\rangle &= H^{\otimes n+1}\,|\psi_0\rangle \\ &= H^{\otimes n}\left|\underline{0}\right\rangle \cdot H\,|1\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}\left|\underline{\ell}\right\rangle \cdot \tfrac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle)\end{aligned}$$

- Oracle.

$$\begin{aligned}|\psi_2\rangle &= O_f\,|\psi_1\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}\left|\underline{\ell}\right\rangle \cdot \tfrac{1}{\sqrt{2}}\left(\left|0\oplus f(\underline{\ell})\right\rangle - \left|1\oplus f(\underline{\ell})\right\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})}\left|\underline{\ell}\right\rangle \cdot \tfrac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle)\end{aligned}$$

On a utilisé :

$$\left|0\oplus f(\underline{\ell})\right\rangle - \left|1\oplus f(\underline{\ell})\right\rangle = \left\{\begin{array}{ll} |0\rangle - |1\rangle & \text{si } f(\underline{\ell}) = 0 \\ -(|0\rangle - |1\rangle) & \text{si } f(\underline{\ell}) = 1 \end{array}\right\} = (-1)^{f(\underline{\ell})}\,(|0\rangle - |1\rangle)\,.$$

- Transformation de Hadamard.

$$\begin{aligned}|\psi_3\rangle &= H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})}\left|\underline{\ell}\right\rangle\right)\cdot\tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\ &= \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})}H^{\otimes n}\left(\left|\underline{\ell}\right\rangle\right)\cdot\tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\ &= \frac{1}{\sqrt{2^n}}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})}\left(\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}(-1)^{\underline{\ell}\odot\underline{k}}\left|\underline{k}\right\rangle\right)\cdot\tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\ &= \frac{1}{2^n}\sum_{k=0}^{2^n-1}\left|\underline{k}\right\rangle\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})+\underline{\ell}\odot\underline{k}}\cdot\tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\end{aligned}$$

Quelle est la probabilité de mesurer $0.0\ldots0$ pour les n premiers qubits ? Il s'agit de trouver le coefficient $\alpha\in\mathbb{C}$ devant le qubit $|0.0\ldots0\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ (le dernier qubit ne sera pas mesuré). Autrement dit il s'agit de trouver le coefficient correspondant à $\underline{k}=\underline{0}$:

$$\alpha=\frac{1}{2^n}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})+\underline{\ell}\odot\underline{0}}.$$

Comme $\underline{\ell}\odot\underline{0}=0$ alors :

$$\alpha=\frac{1}{2^n}\sum_{\ell=0}^{2^n-1}(-1)^{f(\underline{\ell})}.$$

- Si f est constante, par exemple $f(\underline{\ell})=0$, pour tout ℓ, alors :

$$\alpha=\frac{1}{2^n}\sum_{\ell=0}^{2^n-1}(-1)^0=\frac{1}{2^n}\sum_{\ell=0}^{2^n-1}1=1.$$

  Comme le qubit $|\psi_3\rangle$ est normalisé, et que $\alpha=1$ alors les autres coefficients des termes de $|\psi_3\rangle$ sont tous nuls. Ainsi dans ce cas $|\psi_3\rangle=|0.0\ldots0\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ et la probabilité de mesurer $0.0\ldots0$ sur les n premiers qubits est 1.
  De même si f était constante égale à 1, alors on trouverait $\alpha=-1$ et $|\psi_3\rangle=-|0.0\ldots0\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ et la probabilité de mesurer $0.0\ldots0$ sur les n premiers qubits est également 1.
- Si f est équilibrée, il y a autant de ℓ avec $f(\underline{\ell})=0$ que de ℓ avec $f(\underline{\ell})=1$, ainsi il y a autant de ℓ avec $(-1)^{f(\underline{\ell})}=+1$ que $(-1)^{f(\underline{\ell})}=-1$. (On rappelle $(-1)^p=\pm1$.) Ainsi la somme des $(-1)^{f(\underline{\ell})}$ est nulle et donc $\alpha=0$. La probabilité de mesurer $0.0\ldots0$ sur les n premiers qubits est donc 0.

Conclusion : si la mesure sur les n premiers qubits est $0.0\ldots0$ alors la fonction f est constante, sinon c'est qu'elle est équilibrée.