Un premier algorithme quantique

La force de l'informatique quantique est de pouvoir faire des calculs avec des 0 *et des* 1 *en même temps. Au lieu de deux calculs classiques sur le bit* 0*, puis sur le bit* 1*, l'ordinateur quantique effectue un seul calcul sur un* 1*-qubit. Encore plus fort : avec un* n*-qubit, un seul calcul quantique remplace* 2^n *calculs classiques.*
La réalité est cependant plus compliquée, car tous les algorithmes de l'informatique classique ne vont pas miraculeusement être plus rapides grâce à l'informatique quantique. Nous allons voir dans cette partie des problèmes que l'informatique quantique résout beaucoup mieux que les algorithmes classiques. Le but final est de comprendre l'algorithme quantique de Shor qui permet la factorisation rapide des entiers.

Nous commençons par étudier une version simple de l'algorithme de Deutsch–Jozsa afin de nous familiariser avec les objets, les techniques et les types d'algorithmes que nous découvrirons dans cette seconde partie du livre.

1. Objectifs

1.1. Motivation

L'algorithme de Deutsch–Jozsa n'est pas très utile ! Il permet de décider si une fonction est constante ou équilibrée. Cependant cet algorithme est très intéressant car il prouve que l'informatique quantique permet de faire des calculs plus rapidement qu'avec un ordinateur classique.
L'algorithme complet (avec n variables) sera étudié plus loin dans le chapitre « Algorithme de Deutsch–Jozsa ». Dans ce chapitre d'introduction, on se contente de présenter l'algorithme pour les fonctions les plus simples : celles ayant une, puis deux variables.

1.2. Fonction à étudier

On commence par le cas des fonctions d'une seule variable. L'ensemble de départ et d'arrivée est $\{0,1\}$. Considérons une telle fonction :

$$f : \{0,1\} \longrightarrow \{0,1\}$$

Il y a en fait 4 fonctions possibles que l'on sépare en deux catégories :

Fonctions constantes

$$f_0 \begin{cases} 0 & \mapsto & 0 \\ 1 & \mapsto & 0 \end{cases}$$

$$f_1 \begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \end{cases}$$

Fonctions équilibrées

$$f_2 \begin{cases} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \end{cases}$$

$$f_3 \begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{cases}$$

Problème. On nous donne une fonction $f : \{0,1\} \longrightarrow \{0,1\}$, comment déterminer si elle est constante ou équilibrée ?

1.3. Solution classique

La solution classique à ce problème est simple :

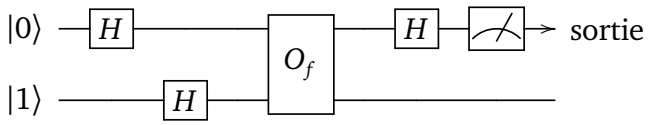
- calculer $f(0)$;
- calculer $f(1)$;
- conclure : si $f(0) = f(1)$ la fonction est constante, sinon elle est équilibrée.

Cet algorithme est très simple, mais il demande deux évaluations de la fonction f (le calcul de $f(0)$ puis celui de $f(1)$) et on ne peut pas faire mieux. Si on définit la complexité de cet algorithme par le nombre d'évaluations de f, alors sa complexité vaut 2.
Nous allons voir un algorithme quantique dont la complexité est 1. Cela ne vous paraît peut-être pas formidablement mieux, mais dans le cas d'une fonction de n variables alors la complexité classique est d'ordre 2^n alors que l'algorithme quantique reste de complexité 1. L'amélioration est donc exponentielle !

2. Circuit quantique

2.1. Circuit

L'algorithme quantique est fourni par le circuit quantique ci-dessous qui répond au problème à l'aide d'une seule évaluation de f.

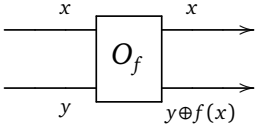


Le circuit est initialisée, puis utilise des portes de Hadamard H mais aussi un sous-circuit O_f, appelé « oracle » que nous détaillerons après.
Algorithme.

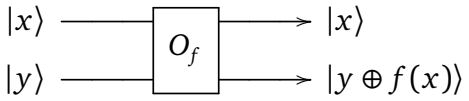
- *Entrée.* Une fonction $f : \{0,1\} \to \{0,1\}$.
- *Sortie.* La sortie est donnée par la mesure sur le premier qubit du circuit. Si la mesure vaut 0, la fonction est constante ; si la mesure vaut 1, la fonction est équilibrée.

2.2. Oracles

Un ***oracle*** est un circuit quantique associé à une fonction f. Voici ce que réalise un oracle pour une fonction $f : \{0,1\} \to \{0,1\}$.



où x et y sont des bits classiques 0 ou 1.
L'oracle nous donne l'action de la porte O_f sur les qubits de base $|0\rangle$ et $|1\rangle$.



Détaillons ce qui se passe sur chaque ligne de l'oracle.

Première ligne. En entrée l'oracle reçoit le bit x et en sortie il renvoie cette même valeur x.
Seconde ligne. En entrée l'oracle reçoit le bit y mais la sortie dépend des valeurs de x, y et de la fonction f. Cette sortie est le bit 0 ou 1, donné par la formule :

$$y \oplus f(x)$$

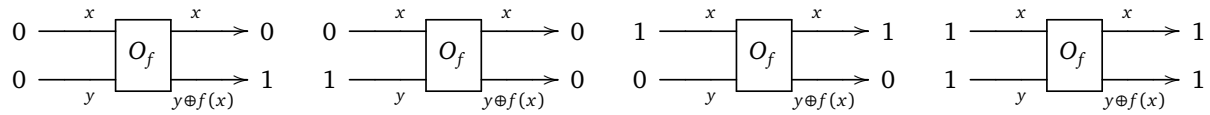
Addition binaire. L'addition « $\oplus$ » est l'addition binaire sur les bits 0 et 1. Elle est équivalent au « ou exclusif » :

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad \boxed{1 \oplus 1 = 0}$$

On rappelle que les valeurs x, y et $f(x)$ valent 0 ou 1. Ainsi la sortie $y \oplus f(x)$ vaut aussi 0 ou 1.

Exemple.
Prenons la fonction f définie par $f(0) = 1$ et $f(1) = 0$.

- Pour $x = 0$, $y = 0$ alors $f(0) = 1$ donc $y \oplus f(x) = 0 \oplus 1 = 1$.
- Pour $x = 0$, $y = 1$ alors $f(0) = 1$ donc $y \oplus f(x) = 1 \oplus 1 = 0$.
- Pour $x = 1$, $y = 0$ alors $f(1) = 0$ donc $y \oplus f(x) = 0 \oplus 0 = 0$.
- Pour $x = 1$, $y = 1$ alors $f(1) = 0$ donc $y \oplus f(x) = 1 \oplus 0 = 1$.



Fonction de deux variables.
Dans notre situation, l'oracle fournit une fonction de deux variables $F : \{0,1\}^2 \to \{0,1\}^2$ définie par :

$$F(x,y) = \big(x, y \oplus f(x)\big).$$

Exemple.
Reprenons la fonction f définie par $f(0) = 1$ et $f(1) = 0$. Alors

$$(0,0) \overset{F}{\mapsto} (0,1) \qquad (0,1) \overset{F}{\mapsto} (0,0) \qquad (1,0) \overset{F}{\mapsto} (1,0) \qquad (1,1) \overset{F}{\mapsto} (1,1)$$

Action sur les qubits.
L'oracle associé à f définit alors une fonction sur les 2-qubits. Notons $\tilde{F} : \mathbb{C}^4 \to \mathbb{C}^4$ définie sur la base canonique $(|0.0\rangle, |0.1\rangle, |1.0\rangle, |1.1\rangle)$ par la fonction F, c'est à dire $\tilde{F}(|x.y\rangle) = |F(x,y)\rangle$, puis étendue par linéarité à $\mathbb{C}^4$. Si

$$|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle\,.$$

Alors :

$$\tilde{F}\big(\,|\psi\rangle\,\big) = \alpha\tilde{F}(|0.0\rangle) + \beta\tilde{F}(|0.1\rangle) + \gamma\tilde{F}(|1.0\rangle) + \delta\tilde{F}(|1.1\rangle).$$

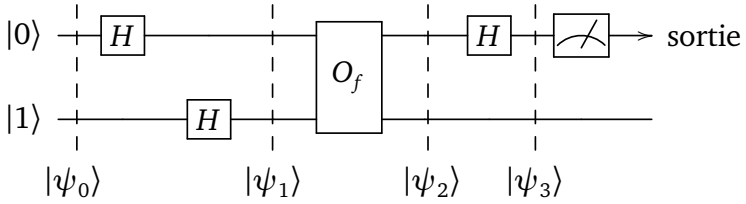
Exemple.
Toujours sur le même exemple, cela donne :

$$|0.0\rangle \overset{\tilde{F}}{\mapsto} |0.1\rangle \qquad |0.1\rangle \overset{\tilde{F}}{\mapsto} |0.0\rangle \qquad |1.0\rangle \overset{\tilde{F}}{\mapsto} |1.0\rangle \qquad |1.1\rangle \overset{\tilde{F}}{\mapsto} |1.1\rangle$$

Et ainsi :

$$\tilde{F}\big(\,|\psi\rangle\,\big) = \beta\,|0.0\rangle + \alpha\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle\,.$$

2.3. Preuve



Nous détaillons les calculs en suivant l'évolution des qubits au fil du circuit.
Qubit initial $|\psi_0\rangle$.

$$|\psi_0\rangle = |0\rangle \otimes |1\rangle = |0.1\rangle$$

Qubit $|\psi_1\rangle$ obtenu après transformation de Hadamard.
On applique une porte de Hadamard sur la première ligne : $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, et une autre sur la seconde ligne $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Ainsi :

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &= \frac{1}{2}\big(\,|0.0\rangle - |0.1\rangle + |1.0\rangle - |1.1\rangle\,\big). \end{aligned}$$

Pour simplifier l'écriture des calculs dans la suite, on va « oublier » le coefficient $\frac{1}{2}$ et écrire 0.0 au lieu de $|0.0\rangle$, 0.1 au lieu de $|0.1\rangle$,... Ainsi on note :

$$|\psi_1\rangle \equiv 0.0 - 0.1 + 1.0 - 1.1$$

Qubit $|\psi_2\rangle$ obtenu après l'oracle.

$$|\psi_2\rangle \equiv 0.(0 \oplus f(0)) - 0.(1 \oplus f(0)) + 1.(0 \oplus f(1)) - 1.(1 \oplus f(1))$$

En effet, l'oracle envoie x sur x pour la première ligne et y sur $y \oplus f(x)$ pour la seconde. Attention « $\oplus$ » est l'addition binaire et doit être effectuée en priorité. Il ne faut pas la confondre avec l'addition de qubits, notée « $+$ » : $x.(y \oplus f(x))$ n'a rien à voir avec $x.(y + f(x))$.
On regroupe les termes commençant par le même qubit :

$$|\psi_2\rangle \equiv \underbrace{0.(0 \oplus f(0)) - 0.(1 \oplus f(0))}_{A} \quad + \quad \underbrace{1.(0 \oplus f(1)) - 1.(1 \oplus f(1))}_{B}.$$

Calculons le terme A en fonction de $f(0)$:

$$A = \begin{cases} 0.0 - 0.1 & \text{si } f(0) = 0 \\ -(0.0 - 0.1) & \text{si } f(0) = 1 \end{cases} \qquad \text{donc} \qquad A = (-1)^{f(0)}(0.0 - 0.1).$$

On rappelle que $(-1)^k$ est juste une façon d'obtenir $+1$ ou -1 selon la parité de k :

$$(-1)^k = \begin{cases} +1 & \text{si } k = 0 \text{ (ou si } k \text{ est pair)} \\ -1 & \text{si } k = 1 \text{ (ou si } k \text{ est impair)} \end{cases}$$

Ainsi :

$$|\psi_2\rangle \equiv (-1)^{f(0)}(0.0 - 0.1) + (-1)^{f(1)}(1.0 - 1.1).$$

Qubit $|\psi_3\rangle$ obtenu après une porte de Hadamard.
Après l'oracle on applique une porte de Hadamard sur la première ligne. Ainsi :

$$\begin{aligned}|\psi_3\rangle &\equiv (-1)^{f(0)}((0+1).0-(0+1).1)\\ &\qquad +(-1)^{f(1)}((0-1).0-(0-1).1)\\ &\equiv (-1)^{f(0)}(0.0-0.1+1.0-1.1)\\ &\qquad +(-1)^{f(1)}(0.0-0.1-1.0+1.1)\\ &\equiv \left((-1)^{f(0)}+(-1)^{f(1)}\right)0.0\\ &\quad +\left(-(-1)^{f(0)}-(-1)^{f(1)}\right)0.1\\ &\quad +\left((-1)^{f(0)}-(-1)^{f(1)}\right)1.0\\ &\quad +\left(-(-1)^{f(0)}+(-1)^{f(1)}\right)1.1\end{aligned}$$

Le coefficient que l'on a omis devant tous les qubits est $\frac{1}{2\sqrt{2}}$ et correspond aux trois portes de Hadamard (chacune apportant un facteur $\frac{1}{\sqrt{2}}$) :

$$|\psi_3\rangle = \frac{1}{2\sqrt{2}}\left((-1)^{f(0)}+(-1)^{f(1)}\right)|0.0\rangle \quad + \quad \cdots$$

Discutons maintenant selon la catégorie de f.

Si f est constante. Alors $f(0)=f(1)$, donc

$$(-1)^{f(0)}+(-1)^{f(1)} = \begin{cases} +2 \\ \text{ou } -2 \end{cases}$$

$$\text{et} \qquad (-1)^{f(0)}-(-1)^{f(1)}=0.$$

Ainsi :

$$|\psi_3\rangle = \pm\tfrac{1}{\sqrt{2}}\left(|0.0\rangle - |0.1\rangle\right)$$

donc la mesure sur le premier qubit donne 0 dans tous les cas, car les seuls 2-qubits présents sont $|0.0\rangle$ et $|0.1\rangle$.

Si f est équilibrée. Alors $f(0)\neq f(1)$, donc

$$(-1)^{f(0)}+(-1)^{f(1)}=0 \qquad \text{et} \qquad (-1)^{f(0)}-(-1)^{f(1)}=\pm 2$$

alors :

$$|\psi_3\rangle = \pm\tfrac{1}{\sqrt{2}}\left(|1.0\rangle - |1.1\rangle\right).$$

La mesure sur le premier qubit donne donc 1 dans tous les cas (car les 2-qubits présents sont $|1.0\rangle$ et $|1.1\rangle$).

Conclusion. Si f est constante la mesure du premier qubit donne 0, si f est équilibrée cette mesure donne 1. Ainsi le circuit répond bien au problème posé et l'oracle associé à f n'a été appelé qu'une seule fois.

2.4. Réalisation des oracles

C'est à celui qui utilise l'algorithme de fournir l'oracle, sorte de boîte noire, utilisée par l'algorithme. Voyons quel circuit quantique permet de réaliser l'oracle O_f pour chacune des quatre possibilités de la fonction f. Notons au préalable que x s'envoie sur x, donc pour la première ligne quantique il n'y a rien à faire.

Fonction constante égale à 0

$$f_0 \begin{cases} 0 & \mapsto & 0 \\ 1 & \mapsto & 0 \end{cases}$$

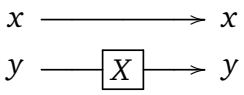
Comme $y \oplus f(x) = y \oplus 0 = y$ alors l'oracle envoie y sur y. Il n'y a rien à faire comme circuit quantique.

$$\begin{array}{ccc} x & \longrightarrow & x \\ y & \longrightarrow & y \end{array}$$

Fonction constante égale à 1

$$f_1 \begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \end{cases}$$

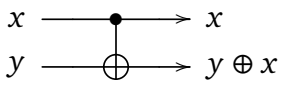
Comme $y \oplus f(x) = y \oplus 1 = NOT(y)$ alors l'oracle envoie y sur $NOT(y)$, que l'on peut réaliser par une porte X.



Fonction équilibrée identité

$$f_2 \begin{cases} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \end{cases}$$

Alors $f_2(x) = x$ et $y \oplus f(x) = y \oplus x$, c'est donc y si $x = 0$ et $NOT(y)$ si $x = 1$. C'est exactement l'action d'une porte $CNOT$:



Fonction équilibrée f_3

$$f_3 \begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{cases}$$

À vous de chercher en exercice un circuit qui réalise cet oracle en vous aidant des deux circuits précédents.

3. Cas de deux variables

3.1. Problème

On considère maintenant une fonction de deux variables :

$$\begin{array}{rccc} f: & \{0,1\}^2 & \longrightarrow & \{0,1\} \\ & (x,y) & \longmapsto & f(x,y) \end{array}$$

On ne s'intéresse qu'à deux catégories de fonctions.

Fonctions constantes. Il y a en a deux :

- f est constante égale à 0 : $f(x,y) = 0 \ \forall x, y \in \{0,1\}$,
- f est constante égale à 1 : $f(x,y) = 1 \ \forall x, y \in \{0,1\}$.

Fonctions équilibrées. Pour ces fonctions, il y a autant de valeurs (x,y) avec $f(x,y) = 0$ que de valeurs avec $f(x,y) = 1$. Il y a 6 fonctions possibles. Voici un exemple :

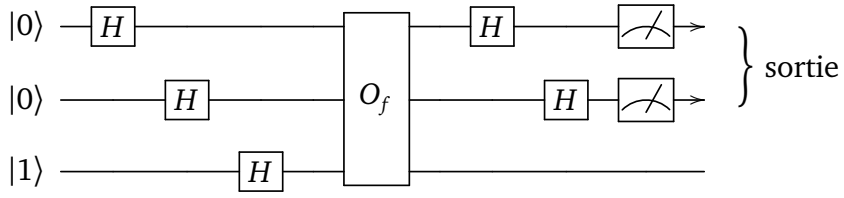
$$(0,0) \overset{f}{\mapsto} 1 \qquad (0,1) \overset{f}{\mapsto} 0 \qquad (1,0) \overset{f}{\mapsto} 0 \qquad (1,1) \overset{f}{\mapsto} 1$$

Attention ! Il existe des fonctions qui ne sont ni constantes, ni équilibrées. Par exemple, la fonction qui vaut 0 partout, sauf en $(1,1)$ ($f(1,1) = 1$).

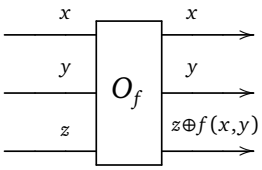
Problème. On nous donne une fonction $f : \{0,1\}^2 \longrightarrow \{0,1\}$ qui a la propriété d'être soit constante, soit équilibrée, mais on ne nous dit pas à quelle catégorie elle appartient. Comment déterminer cette catégorie constante ou équilibrée ?

La solution classique est de calculer plusieurs valeurs. Parfois calculer deux valeurs suffit, par exemple si $f(0,0) \neq f(0,1)$ alors la fonction n'est pas constante, elle est donc équilibrée. Mais si $f(0,0) = f(0,1)$ alors il faut calculer une troisième valeur $f(1,0)$ pour pouvoir conclure. La complexité de l'algorithme classique est de 3 évaluations (on retient toujours le pire cas).

3.2. Circuit solution



Encore une fois, le circuit fait intervenir des portes de Hadamard et un oracle O_f qui dépend de la fonction f dont le circuit quantique est fourni par celui qui pose le problème. Pour nous, c'est une boîte noire :



où x, y, z sont des bits classiques 0 ou 1. La sortie de la troisième ligne est $z \oplus f(x, y)$.
Noter que la mesure se fait sur les deux premières lignes quantiques seulement. La réponse au problème est donnée par cette mesure :

- si la mesure est 0.0 alors la fonction est constante,
- sinon la fonction est équilibrée.

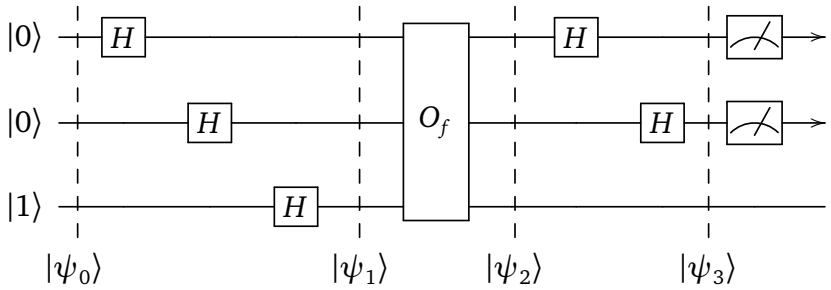
On rappelle que la fonction f doit par hypothèse être dans l'une des deux catégories ci-dessus.
Le circuit quantique n'effectue qu'une seule évaluation de f (plus précisément qu'un seul appel au circuit de l'oracle) et donc la solution proposée est de complexité 1. Cette évaluation correspond à

$$f\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right),$$

qui est une façon d'évaluer f sur les quatre qubits de base $|0.0\rangle$, $|0.1\rangle$, $|1.0\rangle$ et $|1.1\rangle$ simultanément.

3.3. Calcul et preuve

Les calculs et la preuve peuvent être omis lors d'une première lecture, d'une part ils sont similaires à ceux pour une variable (mais un peu plus compliqués) et d'autre part les calculs seront faits dans le cas général d'une fonction de n variables dans le chapitre « Algorithme de Deutsch–Jozsa ».



Qubit initial $|\psi_0\rangle$.

$$|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle = |0.0.1\rangle$$

Qubit $|\psi_1\rangle$. Pour simplifier l'écriture des calculs on « oublie » le coefficient constant commun à tous les qubits.

$$\begin{aligned}|\psi_1\rangle &\equiv (|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)\\ &\equiv |0.0.0\rangle-|0.0.1\rangle\\ &\quad +|0.1.0\rangle-|0.1.1\rangle\\ &\quad +|1.0.0\rangle-|1.0.1\rangle\\ &\quad +|1.1.0\rangle-|1.1.1\rangle\\ &\equiv \sum_{x,y\in\{0,1\}} |x.y.0\rangle-|x.y.1\rangle\end{aligned}$$

Qubit $|\psi_2\rangle$. On applique l'oracle et on va remarquer que

$$|x.y.(0\oplus f(x,y))\rangle-|x.y.(1\oplus f(x,y))\rangle=(-1)^{f(x,y)}(|x.y.0\rangle-|x.y.1\rangle).$$

Ainsi

$$\begin{aligned}|\psi_2\rangle &\equiv \sum_{x,y\in\{0,1\}} |x.y.(0\oplus f(x,y))\rangle-|x.y.(1\oplus f(x,y))\rangle\\ &\equiv \sum_{x,y\in\{0,1\}} (-1)^{f(x,y)}(|x.y.0\rangle-|x.y.1\rangle)\\ &\equiv \sum_{x,y\in\{0,1\}} (-1)^{f(x,y)}|x.y\rangle\,|0-1\rangle\end{aligned}$$

Qubit $|\psi_3\rangle$.

$$\begin{aligned}|\psi_3\rangle &\equiv \sum_{x,y\in\{0,1\}} (-1)^{f(x,y)}|H(x).H(y)\rangle\,|0-1\rangle\\ &\equiv (-1)^{f(0,0)}|0+1\rangle\,|0+1\rangle\,|0-1\rangle\\ &\quad +(-1)^{f(0,1)}|0+1\rangle\,|0-1\rangle\,|0-1\rangle\\ &\quad +(-1)^{f(1,0)}|0-1\rangle\,|0+1\rangle\,|0-1\rangle\\ &\quad +(-1)^{f(1,1)}|0-1\rangle\,|0-1\rangle\,|0-1\rangle\end{aligned}$$

Le troisième qubit est toujours $|0-1\rangle$. On ne va pas expliciter tous les termes mais seulement le coefficient devant le qubit $|0.0.(0-1)\rangle$. On en profite pour remettre les coefficients oubliés :

$$|\psi_3\rangle=\underbrace{\frac{1}{4}\big((-1)^{f(0,0)}+(-1)^{f(0,1)}+(-1)^{f(1,0)}+(-1)^{f(1,1)}\big)}_{\alpha}|0.0\rangle\left|\tfrac{1}{\sqrt{2}}(0-1)\right\rangle \quad + \quad \cdots$$

Conclusion.
Si f est constante alors $\alpha=\pm1$ (ce qui fait qu'il n'y a pas d'autres qubits) et

$$|\psi_3\rangle=\pm|0.0\rangle\left|\tfrac{1}{\sqrt{2}}(0-1)\right\rangle.$$

Ainsi toute mesure sur les deux premiers qubits donne 0.0.
Si f est équilibrée alors il y a autant de valeurs en lesquelles f vaut 0 que de valeurs en lesquelles f vaut 1, donc

$$\alpha=\frac{1}{4}\big((-1)^{f(0,0)}+(-1)^{f(0,1)}+(-1)^{f(1,0)}+(-1)^{f(1,1)}\big)=0.$$

Ainsi $|\psi_3\rangle$ n'a pas de qubits commençant par 0.0. Donc aucune mesure sur les deux premiers qubits ne peut donner 0.0.
Nous avons donc bien résolu notre problème : si la mesure des deux premiers qubits donne 0.0 alors f est constante, sinon f est équilibrée.