CS–308 — Calcul Quantique

Homework IV — François Dumoncel — 314420

Exercise 1 *Algorithme de Deutsch et Josza le plus simple possible*

On considère une fonction d'un bit classique $x \in \{0,1\}$, $x \to f(x)$ ou l'image prend ses valeurs dans $\{0,1\}$. Il existe 4 fonctions de ce type. On veut déterminer si la fonction est constante ou balancée (il y a deux fonctions constantes et deux fonctions balancées). Avec un "circuit classique" pour déterminer si f est constante ou balancée il faut calculer les deux sorties possibles $f(0)$ et $f(1)$ puis les comparer (par exemple on calcule $f(0) - f(1)$ et on détermine si cette différence vaut 0 ou 1). On doit "appeler" la fonction f deux fois. On suppose que l'on a disposition une porte quantique qui effectue l'opération

$$U_f\{|x\rangle \otimes |y\rangle\} = |x\rangle \otimes |y \oplus f(x)\rangle$$

1. Montrez que U_f est une matrice unitaire. *Indication : une matrice est unitaire si et seulement si elle conserve le produit scalaire.*

Solution. Il est facile de voir que la norme d'un vecteur de $\mathbb{C}^2 \otimes \mathbb{C}^2$ est simplement :

$$\| |x\rangle \otimes |y\rangle \|^2 = \| |x\rangle \|^2 \| |y\rangle \|^2$$

Il suffit donc de montrer que

$$\|U_f\{|x\rangle \otimes |y\rangle\}\|^2 = \| |x\rangle \otimes |y\rangle \|^2 = \| |x\rangle \|^2 \| |y\rangle \|^2$$

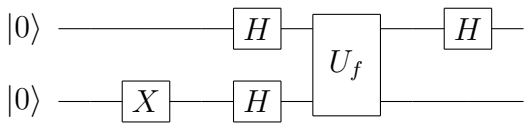
On a

$$\begin{aligned} \|U_f\{|x\rangle \otimes |y\rangle\}\|^2 &= \| |x\rangle \otimes |y \oplus f(x)\rangle \|^2 \\ &= \| |x\rangle \|^2 \times \| |y \oplus f(x)\rangle \|^2 \\ &= \begin{cases} \| |x\rangle \|^2 \| |y\rangle \|^2 & \text{si } f(x) = 0 \\ \| |x\rangle \|^2 \| |\bar{y}\rangle \|^2 & \text{si } f(x) = 1 \end{cases} \end{aligned}$$

Comme $|y\rangle \in \mathbb{F}_2^2$ est un vecteur de bit, il est évident que $\|y\|^2 = \|\bar{y}\|^2$ ce qui montre que U_f est unitaire.

2. Reprendre le circuit de Deutsch et Josza du cours et refaire l'analyse détaillee dans ce cas particulier. Montrez en particulier qu'une seule utilisation de Uf suffit à déterminer si f est constante ou balancée.

Solution. Notre situation se modélise par le circuit suivant



A l'état initial on a simplement $|\Psi_0\rangle = |0\rangle \otimes |0\rangle$.

- Après la porte X :

$$(\mathbb{I} \otimes X) |\Psi_0\rangle = |0\rangle \otimes |1\rangle = |\Psi_1\rangle$$

- Après les portes H :

$$\begin{aligned}(H \otimes H) |\Psi_1\rangle &= H |0\rangle \otimes H |1\rangle \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}} \sum_{b=0,1} |b\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= |\Psi_2\rangle\end{aligned}$$

- Après U_f

$$\begin{aligned}U_f |\Psi_2\rangle &= \frac{1}{\sqrt{2}} \sum_{b=0,1} \left(\frac{1}{\sqrt{2}} U_f |b0\rangle - \frac{1}{\sqrt{2}} U_f |b1\rangle \right) \\ &= \frac{1}{\sqrt{2}} \sum_{b=0,1} \left(\frac{1}{\sqrt{2}} |bf(b)\rangle - \frac{1}{\sqrt{2}} |b\overline{f(b)}\rangle \right)\end{aligned}$$

  On peut maintenant regarder ce qu'il se passe si f prend les valeurs $0, 1$:

  - $\forall x \in \mathbb{F}_2, f(x) = 0$.

$$\frac{1}{\sqrt{2}} \sum_{b=0,1} \left(\frac{1}{\sqrt{2}} |b0\rangle - \frac{1}{\sqrt{2}} |b1\rangle \right) = \frac{1}{\sqrt{2}} \sum_{b=0,1} |b\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

  - $\forall x \in \mathbb{F}_2, f(x) = 1$.

$$\frac{1}{\sqrt{2}} \sum_{b=0,1} \left(\frac{1}{\sqrt{2}} |b1\rangle - \frac{1}{\sqrt{2}} |b0\rangle \right) = \frac{1}{\sqrt{2}} \sum_{b=0,1} |b\rangle \otimes - \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

    On en déduit donc, que de manière générale

$$U_f |\Psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{b=0,1} |b\rangle \otimes (-1)^{f(b)} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{b=0,1} (-1)^{f(b)} |b\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = |\Psi_3\rangle$$

- Après la porte H

$$\begin{aligned}(H \otimes \mathbb{I}) |\Psi_3\rangle &= \frac{1}{\sqrt{2}} \sum_{b=0,1} (-1)^{f(b)} H |b\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}} \sum_{b=0,1} (-1)^{f(b)} \left\{ \frac{1}{\sqrt{2}} \sum_{c=0,1} (-1)^{bc} |c\rangle \right\} \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\end{aligned}$$

$$= \sum_{c=0,1} \left\{ \frac{1}{2} \sum_{b=0}^{1} (-1)^{f(b)} (-1)^{bc} \right\} |c\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$
$$= |\Psi_{fin}\rangle$$

Maintenant, lors de la mesure le premier qubit va être projeté sur un état de la base computationelle $\{|0\rangle, |1\rangle\}$. On a alors que pour $c \in \{0, 1\}$

$$\begin{aligned}
\mathbb{P}(c) &= \left| \frac{1}{2} \sum_{b=0}^{1} (-1)^{f(b)} (-1)^{bc} \right|^2 \\
&= \frac{1}{4} \left| (-1)^{f(0)} + (-1)^{f(1)} (-1)^{c} \right|^2 \\
&= \begin{cases} \frac{1}{4} |(-1)^{f(0)} + (-1)^{f(1)}|^2 & \text{si } c = 0 \\ \frac{1}{4} |(-1)^{f(0)} - (-1)^{f(1)}|^2 & \text{si } c = 1 \end{cases}
\end{aligned}$$

On observe que si f est balancée alors la probabilité d'observer $c = 0$ devient nulle. Si f est constante on observe en revanche que la probabilité d'observer $c = 1$ devient 1. On retrouve donc bien le problème de Deutsch-Josza.

Exercise 2 *Vérifications de calculs (qui reviennent souvent).*

On adopte la notation $|b\rangle, |c\rangle$ pour les états de la base canonique (c.à.d que $b = 0, 1$ et $c = 0, 1$)

1. Vérifiez

$$H |b\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^b |1\rangle) = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{bc} |c\rangle$$

et vérifiez pour $n = 2$

$$H^{\otimes n} |0_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{(b_1,\ldots,b_n) \in \mathbb{F}_2^n} |b_1, \ldots, b_n\rangle$$

$$H^{\otimes n} |b_1, \ldots, b_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{(c_1,\ldots,c_n)} (-1)^{\sum_{i=1}^{n} b_i c_i} |c_1, \ldots, c_n\rangle \tag{1}$$

Solution. Trivial.

2. Prouvez la dernière formule dans le cas n général.

Solution. On procède par récurrence sur n.

- **Initialisation.** Pour $n = 1$ on a

$$H^{\otimes 1} |b_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{b_1} |1\rangle) = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{b_1 c} |c\rangle = \frac{1}{\sqrt{2^1}} \sum_{c_1} (-1)^{\sum_{i=0}^{1} b_i c_i} |c_1\rangle$$

et la formule est donc vraie pour $n = 1$.

- **Hérédité.** Soit $n \geq 2$. On suppose la formule (1) vraie pour $n \in \mathbb{N}$. Montrons que cela implique que (1) est vraie pour $n+1 \in \mathbb{N}$

$$\begin{aligned} H^{\otimes n+1} |b_1, \ldots, b_n, b_{n+1}\rangle &= H^{\otimes n} |b_1, \ldots, b_n\rangle \otimes H |b_{n+1}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{(c_1,\ldots,c_n)} (-1)^{\sum_{i=1}^n b_i c_i} |c_1, \ldots, c_n\rangle \otimes H |b_{n+1}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{(c_1,\ldots,c_n)} (-1)^{\sum_{i=1}^n b_i c_i} |c_1, \ldots, c_n\rangle \otimes \frac{1}{\sqrt{2}} \sum_{c_{n+1}=0}^{1} (-1)^{b_{n+1} c_{n+1}} |c_{n+1}\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{(c_1,\ldots,c_n,c_{n+1})} (-1)^{\sum_{i=1}^{n+1} b_i c_i} |c_1, \ldots, c_n, c_{n+1}\rangle \end{aligned}$$

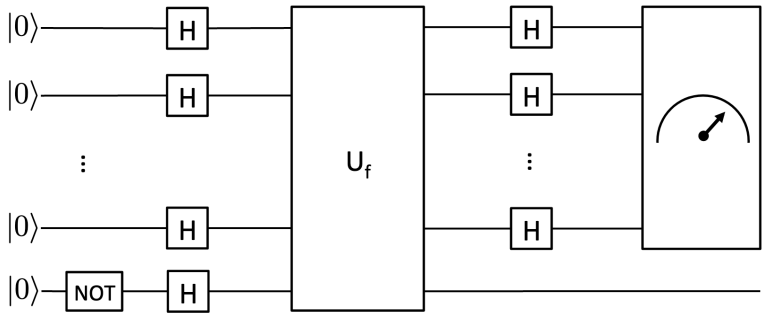
- **Conclusion.** Par l'axiome de récurrence, on a donc que la formule (1) est vraie pour tout $n \geq 1$.

Exercise 3 *Algorithme de Bernstein-Vazirani.*

En 1993 E. Bernstein et U. Vazirani (Proc, 25th Annual ACM Symposium on the Theory of Computing, ACM Press, NY p11-20) formulèrent le problème suivant. Soit $\underline{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ des vecteurs binaires à n composantes. On se donne un "oracle" qui calcule

$$f(\underline{x}) = b \oplus (\underline{a} \cdot \underline{x}) \pmod 2$$

où $b \in \mathbb{F}_2$ et $\underline{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$ et $\underline{a} \cdot \underline{x} = \sum_{i=1}^n a_i x_i$. Le but est de calculer $\underline{a}$ en posant le moins de questions possibles à l'oracle : pour fixer les idées on suppose b connu et $\underline{a}$ inconnu. On considère le circuit de Deutsch et Josza :



1. Calculez l'état de sortie du circuit - juste avant l'appareil de mesure - quand tous les qubits d'entrée sont dans l'état $|0\rangle$. Il est utile de remarquer que $|f(\underline{x})\rangle - |1 \oplus f(\underline{x})\rangle = (-1)^{f(\underline{x})}(|0\rangle - |1\rangle)$.

Solution. Un long calcul donne

$$\begin{aligned} |\Psi_{\text{fin}}\rangle &= H^{\otimes n} |0 \ldots 0\rangle \otimes H |1\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |x_1, \ldots, x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} \left\{ \frac{1}{\sqrt{2}} U_f \left| x_1, \ldots, x_n, 0 \right\rangle - \frac{1}{\sqrt{2}} U_f \left| x_1, \ldots, x_n, 1 \right\rangle \right\} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} \left\{ \frac{1}{\sqrt{2}} \left| x_1, \ldots, x_n, f(\underline{x}) \right\rangle - \frac{1}{\sqrt{2}} \left| x_1, \ldots, x_n, 1 \oplus f(\underline{x}) \right\rangle \right\} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} \left| x_1, \ldots, x_n \right\rangle \otimes \frac{\left| f(\underline{x}) \right\rangle - \left| 1 \oplus f(\underline{x}) \right\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} \left| x_1, \ldots, x_n \right\rangle \otimes (-1)^{f(\underline{x})} \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{f(\underline{x})} \left| x_1, \ldots, x_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{f(\underline{x})} H^{\otimes n} \left| x_1, \ldots, x_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{f(\underline{x})} \left\{ \frac{1}{\sqrt{2^n}} \sum_{\underline{y}} (-1)^{\underline{x} \cdot \underline{y}} \left| y_1, \ldots, y_n \right\rangle \right\} \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{2^n} \sum_{\underline{x}} \sum_{\underline{y}} (-1)^{f(\underline{x})} (-1)^{\underline{x} \cdot \underline{y}} \left| y_1, \ldots, y_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{2^n} \sum_{\underline{x}} \sum_{\underline{y}} (-1)^{f(\underline{x}) + \underline{x} \cdot \underline{y}} \left| y_1, \ldots, y_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{2^n} \sum_{\underline{x}} \sum_{\underline{y}} (-1)^{b \oplus \underline{a} \cdot \underline{x} + \underline{x} \cdot \underline{y}} \left| y_1, \ldots, y_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \\
&= \frac{1}{2^n} \sum_{\underline{x}} \sum_{\underline{y}} (-1)^{b \oplus (\underline{a} + \underline{y}) \cdot \underline{x}} \left| y_1, \ldots, y_n \right\rangle \otimes \frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}}
\end{aligned}
$$

2. Grâce à l'appareil de mesure on fait *une seule mesure* dans la base computationelle des n premiers qubits de sortie du circuit. Montrer que cela suffit à déterminer le vecteur $\underline{a}$ avec probabilité 1.

Solution. On calcule les probabilités pour chaque états de la base canonique

$$
\begin{aligned}
\mathbb{P}(y_1 \ldots y_n) &= \left| \frac{1}{2^n} \sum_{\underline{x}} (-1)^{b \oplus (\underline{a} + \underline{y}) \cdot \underline{x}} \right|^2 \\
&= \frac{1}{4^n} \underbrace{(-1)^{2b}}_{=1} \left| \sum_{\underline{x}} (-1)^{(\underline{a} + \underline{y}) \cdot \underline{x}} \right|^2 \\
&= \frac{1}{4^n} \left| \sum_{\underline{x}} (-1)^{\sum_{i=1}^{n} (a_i + y_i) x_i} \right|^2
\end{aligned}
$$

Pour obtenir une probabilité égal à 1, on doit avoir l'exposant de (-1) toujours égal à 0, ce qui

arrive si

$$(a_i + y_i)x_i = \begin{cases} x_i = 0 \\ \text{ou} \\ a_i = -y_i = y_i \text{ car on est dans } \mathbb{F}_2 \end{cases}$$

Par conséquent on a que

$$\mathbb{P}(y_1 \dots y_n) = \begin{cases} 1 & \text{si } \underline{y} = \underline{a} \\ 0 & \text{sinon.} \end{cases}$$

Par conséquent, peut importe ce qu'on observe on aura toujours que $|y_1 \dots y_n\rangle = |a_1 \dots a_n\rangle$.

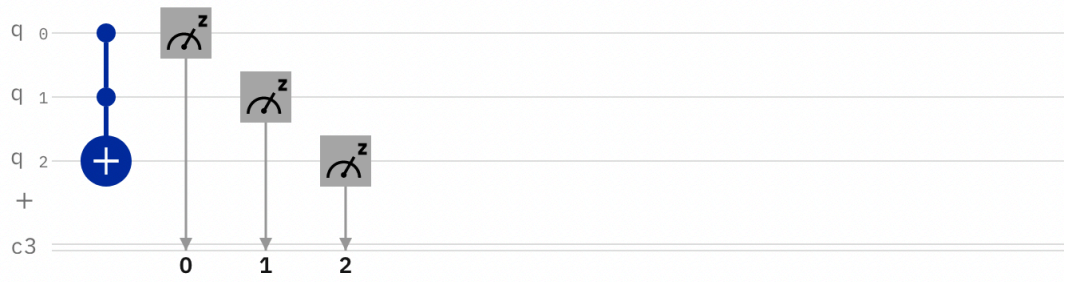
3. A-t-on besoin de savoir la valeur de b pour le succès de l'algorithme ? Si celle-ci n'est pas connue, est-ce que cet algorithme permet de la déterminer ? Justifiez.

Solution. Dans le calcul de probabilité, la carré détruit totalement la présence de b ce qui empêche l'algorithme de pouvoir le déterminer. On peut en revanche exécuter l'algorithme avec succès sans pour autant connaître b.

Exercise 4 *IBM Q practice. Implémentation de la porte de Toffoli*

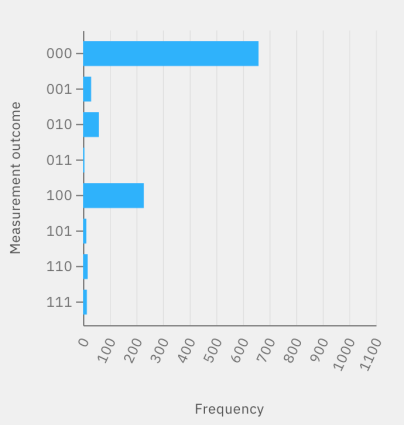
1. On vous demande de tester cette identité avec le composer d'IBM Q. Pour plusieures entrées de votre choix (par exemple $|000\rangle, |110\rangle, |111\rangle$) produisez l'histogramme des mesures pour la porte de Toffoli gauche et pour le circuit quantique droite avec 1024 shots. Vous utiliserez un simulateur et également une machine de votre choix.

Solution. Premier circuit

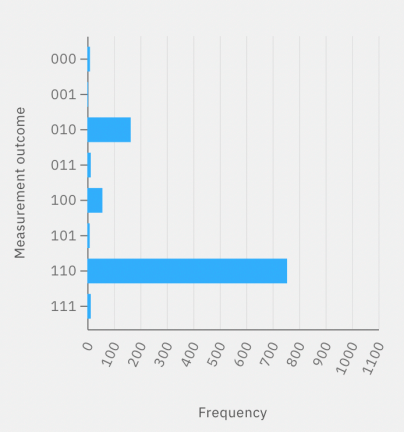


Entrées :

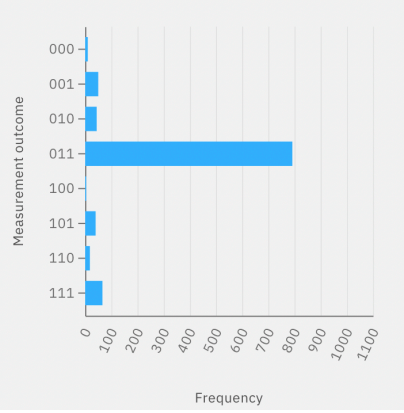
- $|000\rangle$:



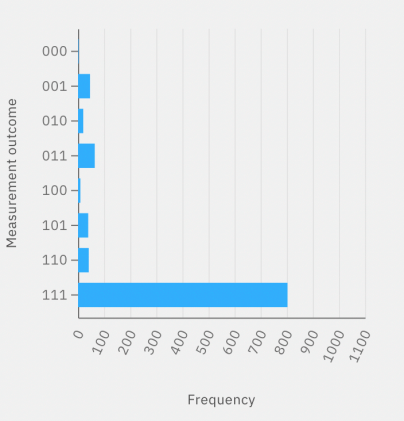
- $|011\rangle$:



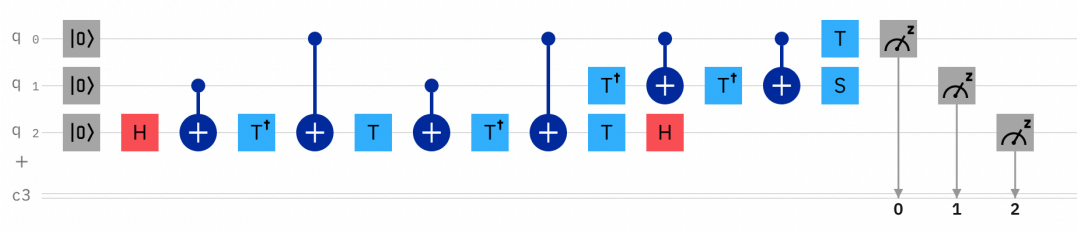
- $|111\rangle$:



- $|110\rangle$:

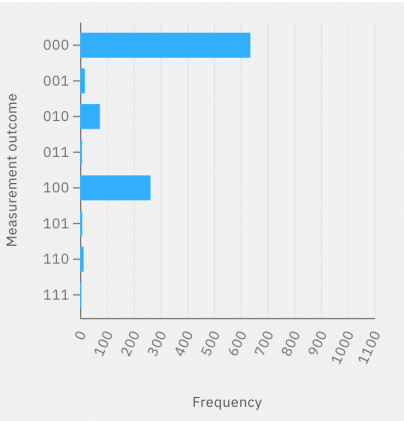


Second circuit :

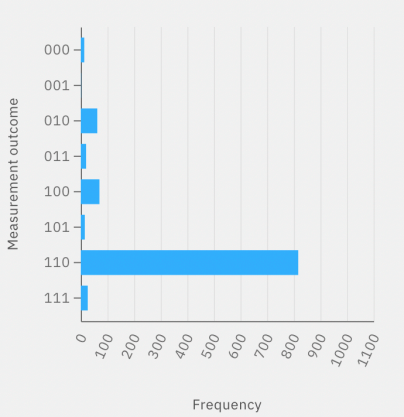


Entrées :

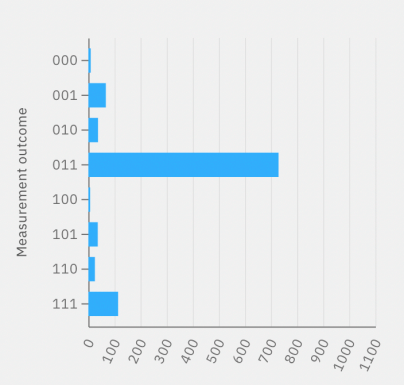
- $|000\rangle$:



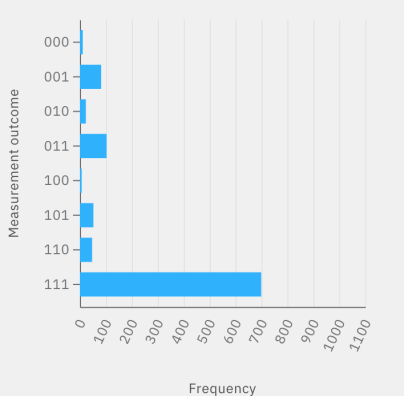
- $|011\rangle$:



- $|111\rangle$:



- $|110\rangle$:



Note : sur les machines d'IBM Q les strings binaires doivent être lus de droite à gauche. En faisant attention à cela on constate bien que les deux circuits sont équivalents.