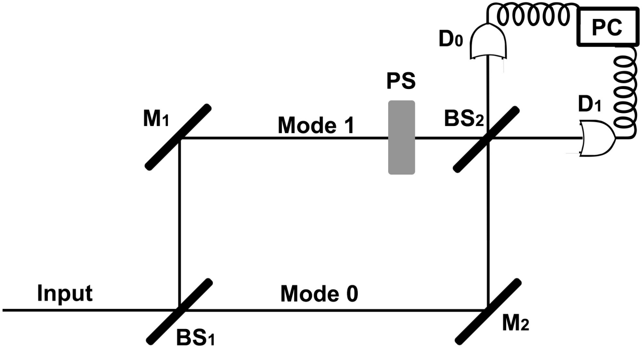
Algoritmos Cuánticos I

Federico Holik

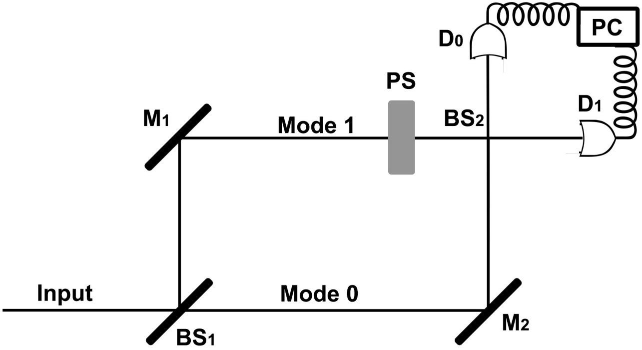
I F L P
CONICET
U N L P

Curso UNAHUR
18/11/2025

Outline


PC
D0
PS
D1
M1
Mode 1
BS2
Input
Mode 0
BS1
M2

Mach-Zender: medición de camino



Descripción matemática de lo que pasa

Brazo de abajo (Modo **0**):

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1}$$

Brazo de arriba (Modo **1**):

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

Los dos separadores de haz se representan por la matriz:

$$BS_1 = BS_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{3}$$

y el phase shifter viene dado por:

$$PS = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\Delta \end{pmatrix} \tag{4}$$

A la salida del primer divisor de haz:

$$|\psi_1\rangle = BS_1|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{i}{\sqrt{2}}\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \tag{5}$$

Luego, opera el phase shifter (cambiador de fase):

$$|\psi_2\rangle = PS|\psi_1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Delta} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + ie^{i\Delta}|1\rangle) \tag{6}$$

Finalmente, aplico el segundo divisor de haz:

$$|\psi_3\rangle = BS_2|\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{ie^{i\Delta}}{\sqrt{2}}\end{pmatrix} = \begin{pmatrix}\frac{1}{2}(1-e^{i\Delta})\\ \frac{i}{2}(1+e^{i\Delta})\end{pmatrix} = \tag{7}$$

$$\frac{1}{2}((1-e^{i\Delta})|0\rangle + i(1+e^{i\Delta})|1\rangle) \tag{8}$$

El estado final queda:

$$|\psi_3\rangle = \frac{1}{2}((1 - e^{i\Delta})|0\rangle + i(1 + e^{i\Delta})|1\rangle) \tag{9}$$

$$|\psi_3\rangle = \frac{e^{i\frac{\Delta}{2}}}{2}((e^{-i\frac{\Delta}{2}} - e^{i\frac{\Delta}{2}})|0\rangle + i(e^{-i\frac{\Delta}{2}} + e^{i\frac{\Delta}{2}})|1\rangle) \tag{10}$$

$$|\psi_3\rangle = \frac{e^{i\frac{\Delta}{2}}}{2}((e^{-i\frac{\Delta}{2}} - e^{i\frac{\Delta}{2}})|0\rangle + i(e^{-i\frac{\Delta}{2}} + e^{i\frac{\Delta}{2}})|1\rangle) \tag{11}$$

$$|\psi_3\rangle = ie^{i\frac{\Delta}{2}}((-\sin(\frac{\Delta}{2}))|0\rangle + (\cos(\frac{\Delta}{2}))|1\rangle) \tag{12}$$

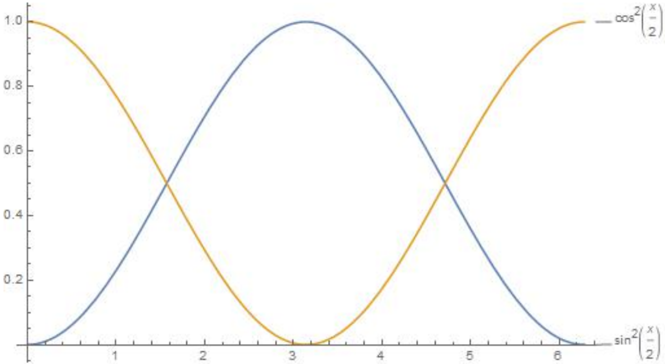
Uso que $e^{i\frac{\Delta}{2}} = \cos(\frac{\Delta}{2}) + i\sin(\frac{\Delta}{2})$:
$e^{-i\frac{\Delta}{2}} - e^{i\frac{\Delta}{2}} = -2i\sin(\frac{\Delta}{2})$
$e^{-i\frac{\Delta}{2}} + e^{i\frac{\Delta}{2}} = 2\cos(\frac{\Delta}{2})$

Por ende, las probabilidades de detección en D_1 y D_2 vienen dadas por:

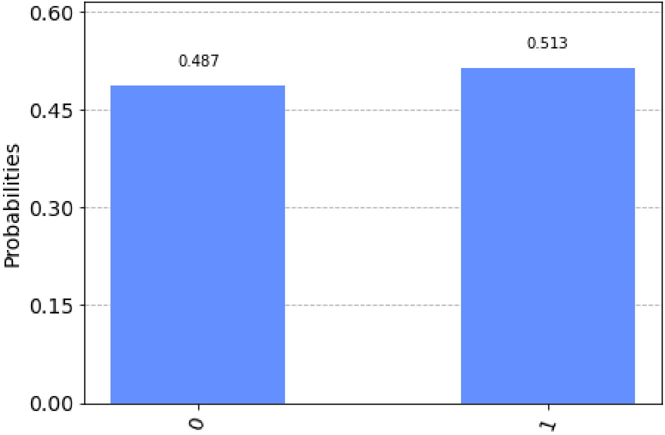
$$P_0 = |\langle 0|\psi_3\rangle|^2 = \sin^2(\frac{\Delta}{2}) \tag{13}$$

$$P_1 = |\langle 1|\psi_3\rangle|^2 = \cos^2(\frac{\Delta}{2}) \tag{14}$$

Gráfico de las cuentas de fotones en función de la fase

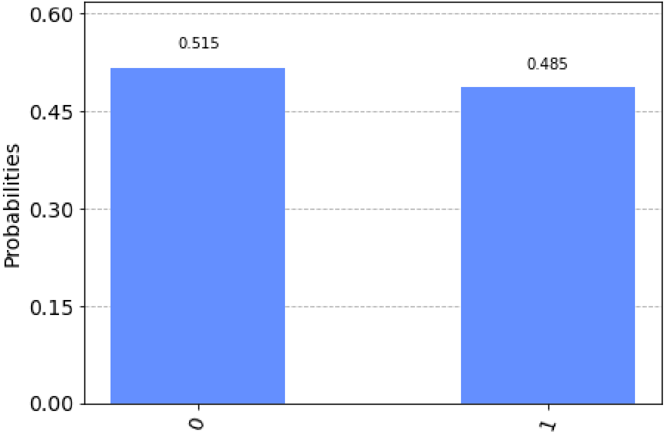


Photon counts: '0': 487, '1': 513



$$|\psi_3\rangle = ie^{i\frac{\pi}{4}}(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \tag{15}$$

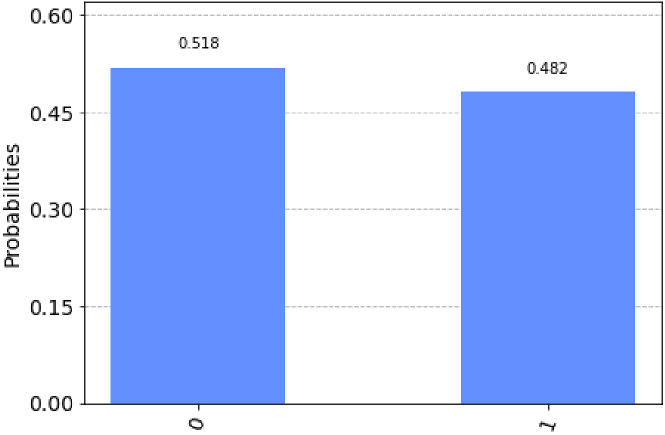
Photon counts: '0': 515, '1': 485



$$|\psi_3\rangle = ie^{i\frac{\pi}{4}}(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \quad (16)$$

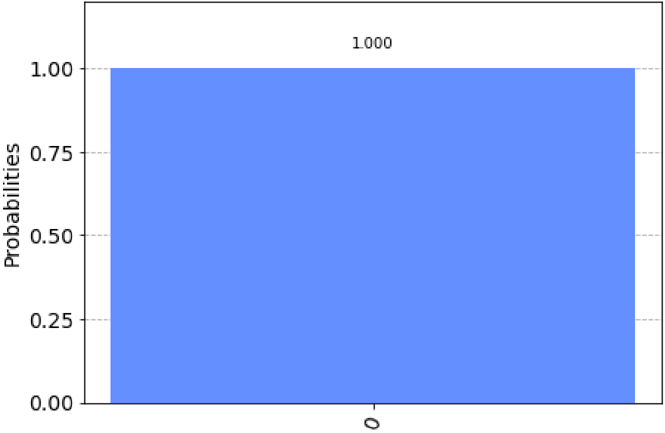
Cuentas de fotones para 1000 corridas ($\Delta = \frac{\pi}{2}$)

Photon counts: '0': 518, '1': 482



$$|\psi_3\rangle = ie^{i\frac{\pi}{4}}(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \tag{17}$$

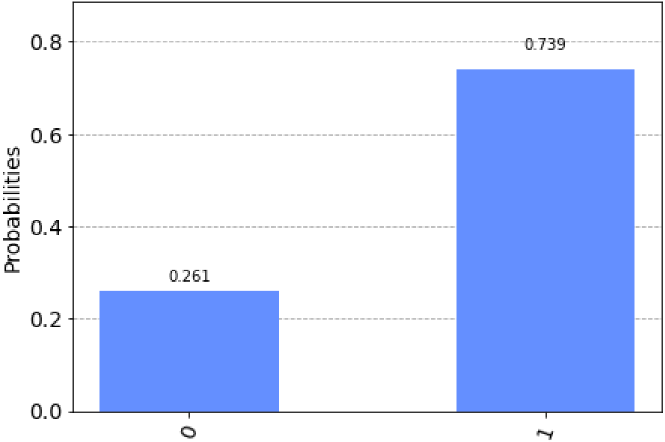
Photon counts: '0': 1000



$$|\psi_3\rangle = -ie^{i\frac{\pi}{2}}|0\rangle \tag{18}$$

Cuentas de fotones para 1000 corridas ($\Delta = \frac{\pi}{3}$)

Photon counts: '0': 261, '1': 739



$$|\psi_3\rangle = ie^{i\frac{\pi}{6}}((-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle) \quad (19)$$

Si, por el contrario, hubiésemos implementado el contexto de detección de caminos, sólo tendríamos $|\psi_2\rangle$, y las probabilidades vendrían dadas por:

$$P_0 = |\langle 0|\psi_2\rangle|^2 = \frac{1}{2} \tag{20}$$

$$P_1 = |\langle 1|\psi_2\rangle|^2 = \frac{1}{2} \tag{21}$$

Si tenemos un qubit:

$$B = \{|0\rangle, |1\rangle\}$$

Si tenemos dos qubits:

$$B = \{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$$
$$B = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Si tenemos tres qubits:

$$B = \{|000\rangle, |100\rangle, |010\rangle, |001\rangle, |110\rangle, |101\rangle, |011\rangle, |111\rangle\}$$

Si tenemos cuatro qubits...

Con dos qubits:
$\langle 00|00\rangle = 1$
$\langle 00|11\rangle = 0$
$\langle 10|10\rangle = 1$
$\langle 10|01\rangle = 0$
Con tres qubits:
$\langle 100|010\rangle = 0$
$\langle 101|101\rangle = 1$

Moraleja: cuando es la misma cadena (de ceros y unos), el producto escalar da uno. Si no, da cero.

$|\psi\rangle = (H^{\otimes n})|0\rangle^{\otimes n} = H|0\rangle \otimes H|0\rangle \ldots \otimes H|0\rangle$

Con dos qubits:

$$|\psi\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Con tres qubits:

$$|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle+|100\rangle+|010\rangle+|001\rangle+|110\rangle+|101\rangle+|011\rangle+|111\rangle)$$

Con n qubits:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}(|0\ldots0\rangle + |010\ldots\rangle + \ldots + |1\ldots1\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

Atención: si $x \in \{0, 1\}^n$, entonces x es una lista de n ceros y unos (y en $\{0, 1\}^n$ hay 2^n listas).

$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = H|0\rangle \otimes H|0\rangle \ldots \otimes H|0\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}(|0\ldots0\rangle + |010\rangle \ldots + |1\ldots1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

Atención: si $y \in \{0,1\}^n$, entonces y es una lista de n ceros y unos (y en $\{0,1\}^n$ hay 2^n listas).

Ejemplo: $|y\rangle = |010110,\ldots,01001\rangle$

$$|\psi\rangle = H^{\otimes n}|y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{yx}|x\rangle$$

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

$$(H \otimes H)|00\rangle = (H|0\rangle) \otimes (H|0\rangle) =$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{4}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$(H \otimes \ldots H)|0 \ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$|\psi\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
Notar que:

$$p_{|10\rangle\langle 10|} = |\langle 10|\psi\rangle|^2 = \frac{1}{4}$$

Y si tenemos:

$$|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle+|100\rangle+|010\rangle+|001\rangle+|110\rangle+|101\rangle+|011\rangle+|111\rangle)$$

$$p_{|101\rangle\langle 101|} = |\langle 101|\psi\rangle|^2 = |\frac{1}{\sqrt{8}}|^2 = \frac{1}{8}$$

$f:\{0,1\}^n \longrightarrow \{0,1\}$ es constante si $f(x)=0$ para todo x, o $f(x)=1$ para todo x.

$f:\{0,1\}^n \longrightarrow \{0,1\}$ es balanceada si la mitad de las veces $f(x)=0$, y $f(x)=1$ la otra mitad.

Ejemplo: $f:\{0,1\} \longrightarrow \{0,1\}$.
$f(0)=1$
$f(1)=0$
es balanceada.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es constante si $f(x) = 0$ para todo x, o $f(x) = 1$ para todo x.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es balanceada si la mitad de las veces $f(x) = 0$, y $f(x) = 1$ la otra mitad.

Ejemplo: $f : \{0,1\} \longrightarrow \{0,1\}$.
$f(0) = 0$
$f(1) = 0$
es constante.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es constante si $f(x) = 0$ para todo x, o $f(x) = 1$ para todo x.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es balanceada si la mitad de las veces $f(x) = 0$, y $f(x) = 1$ la otra mitad.

Ejemplo: $f : \{0,1\} \longrightarrow \{0,1\}$.
$f(0) = 0$
$f(1) = 1$
es balanceada.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es constante si $f(x) = 0$ para todo x, o $f(x) = 1$ para todo x.

$f : \{0,1\}^n \longrightarrow \{0,1\}$ es balanceada si la mitad de las veces $f(x) = 0$, y $f(x) = 1$ la otra mitad.

Ejemplo: $f : \{0,1\} \longrightarrow \{0,1\}$.
$f(0) = 1$
$f(1) = 1$
es constante.

Funciones $f_i : \{0,1\} \longrightarrow \{0,1\}$:

$$\begin{array}{ll} f_1(0) = 0 & f_1(1) = 1 \\ f_2(0) = 1 & f_2(1) = 0 \\ f_3(0) = 0 & f_3(1) = 0 \\ f_4(0) = 1 & f_4(1) = 1 \end{array} \tag{22}$$

Hay dos clases: $C = \{f_1, f_2\}$ y $B = \{f_3, f_4\}$, y hay que determinar si f pertenece a B o a C (bajo la premisa de que pertenece a alguna de las dos).

Problema: supongamos que tenemos una $f : \{0,1\}^n \longrightarrow \{0,1\}$, y sabeemos que es constante o balanceada (pero no sabemos cual de las posibilidades ocurre).

Queremos determinar si es constante o balanceada *haciendo la menor cantidad de evaluaciones posibles* de la función (consultando a un "oráculo" que nos puede decir cuánto vale la función en un input dado).

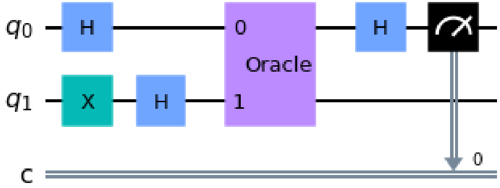
Primero lo hacemos con dos qubits (para una $f : \{0,1\} \longrightarrow \{0,1\}$).
Inicializamos en:

$$|\psi_0\rangle = |01\rangle$$

y luego, aplicamos Hadamards:

$$|\psi_1\rangle = (H \otimes H)|01\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$|\psi_1\rangle = (H \otimes H)|01\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$



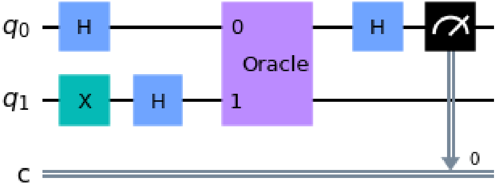
Primer paso: aplico Hadamard al primer qubit y X + Hadamard al segundo.

Algoritmo de Deutsch-Jozsa: Paso 2

Aplicamos una implementación cuántica de f:

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

$$\begin{aligned}
|0\rangle|0\rangle &\xrightarrow{U_f} |0\rangle|0 \oplus f(0)\rangle \\
|0\rangle|1\rangle &\xrightarrow{U_f} |0\rangle|1 \oplus f(0)\rangle \\
|1\rangle|0\rangle &\xrightarrow{U_f} |1\rangle|0 \oplus f(1)\rangle \\
|1\rangle|1\rangle &\xrightarrow{U_f} |1\rangle|1 \oplus f(1)\rangle
\end{aligned}$$



Segundo paso: aplico el oráculo.

Algoritmo de Deutsch-Jozsa: Paso 2

$$|\psi_1\rangle = (H \otimes H)|01\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2^2}}(U_f|0\rangle|0\rangle - U_f|0\rangle|1\rangle + U_f|1\rangle|0\rangle - U_f|1\rangle|1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle(|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|f(1)\rangle - |1 \oplus f(1)\rangle))$$

$$|f(0)\rangle - |1 \oplus f(0)\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$$
$$|f(1)\rangle - |1 \oplus f(1)\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle)$$

Algoritmo de Deutsch-Jozsa: Paso 2

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle((-1)^{f(0)}(|0\rangle - |1\rangle)) + |1\rangle(-1)^{f(1)}(|0\rangle - |1\rangle))$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(-1)^{f(0)}(|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)\oplus f(0)}|1\rangle(0\rangle - |1\rangle)))$$

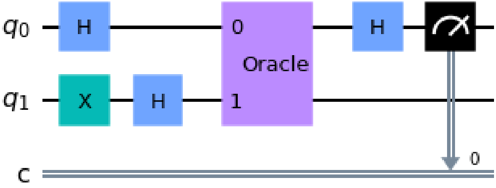
$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(-1)^{f(0)}(|0\rangle + (-1)^{f(1)\oplus f(0)}|1\rangle)(|0\rangle - |1\rangle)$$

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(1)\oplus f(0)}|1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}(-1)^{f(0)}(|0\rangle + (-1)^{f(1)\oplus f(0)}|1\rangle))(|0\rangle - |1\rangle)$$

$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(1)\oplus f(0)}|1\rangle)$$

$$H|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + (-1)^{f(1)\oplus f(0)}H|1\rangle)$$



Tercer paso: aplico Hadamard al primer qubit.

Algoritmo de Deutsch-Jozsa: Paso 3

$|\psi_3\rangle = H|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + (-1)^{f(1)\oplus f(0)}H|1\rangle)$

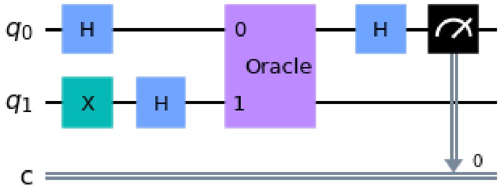
Recuerden:

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}^2}(|0\rangle + |1\rangle + (-1)^{f(1)\oplus f(0)}|0\rangle - (-1)^{f(1)\oplus f(0)}|1\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}^2}((1 + (-1)^{f(1)\oplus f(0)})|0\rangle + (1 - (-1)^{f(1)\oplus f(0)})|1\rangle)$$



Cuarto paso: medimos en el primer qubit.

Algoritmo de Deutsch-Jozsa: Paso 4

$|\psi_3\rangle = \frac{1}{2}((1 + (-1)^{f(1)\oplus f(0)})|0\rangle + (1 - (-1)^{f(1)\oplus f(0)})|1\rangle)$

$f(0) \oplus f(1) = 0$ (ocurre siempre que f sea constante)

$f(0) \oplus f(1) = 1$ (ocurre siempre que f sea balanceada)

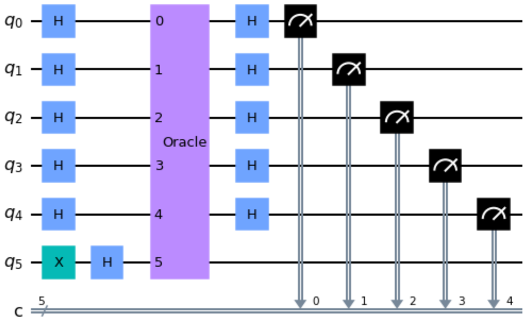
Si mido y obtengo $|0\rangle$, concluyo que es constante. De lo contrario, conluyo que es balanceada.

Observación importante: sólo tuvimos que aplicar el oráculo una vez.

Problema: supongamos que tenemos una $f : \{0,1\}^n \longrightarrow \{0,1\}$, y sabeemos que es constante o balanceada (pero no sabemos cual de las posibilidades ocurre).

Queremos determinar si es constante o balanceada haciendo la menor cantidad de evaluaciones posibles (consultando a un “oráculo” que nos puede decir cuánto vale la función en un input dado).

Esquema del circuito

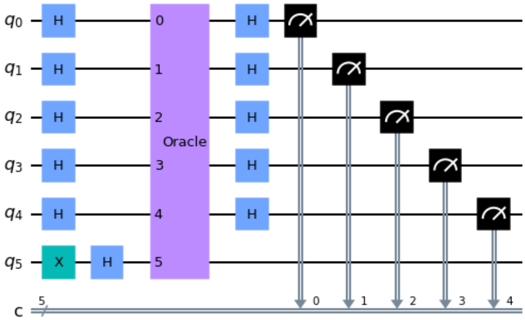


Primer paso: aplico Hadamard a los primeros qubits y X + Hadamard al último.

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle = |0\rangle \otimes \ldots \otimes |0\rangle \otimes |1\rangle$$

$$|\psi_1\rangle = (H^{n+1})(|0\rangle \otimes \ldots \otimes |0\rangle \otimes |1\rangle)$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$



Segundo paso: aplico el oráculo.

$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$
Aplico una implementación cuántica de la función f:
$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$

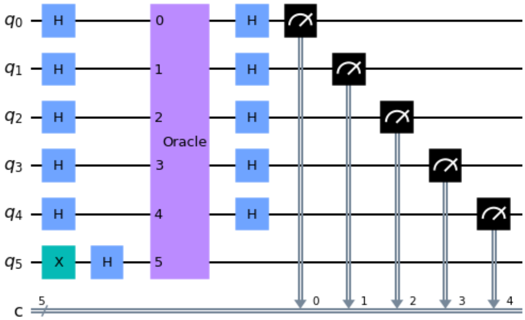
$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} U_f|x\rangle(|0\rangle - |1\rangle)$$

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

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}(\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle)(|0\rangle - |1\rangle)$$

$$|\widetilde{\psi_2}\rangle = \frac{1}{\sqrt{2^{n}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle$$



Tercer paso: vuelvo a aplicar Hadamard a los primeros n qubits.

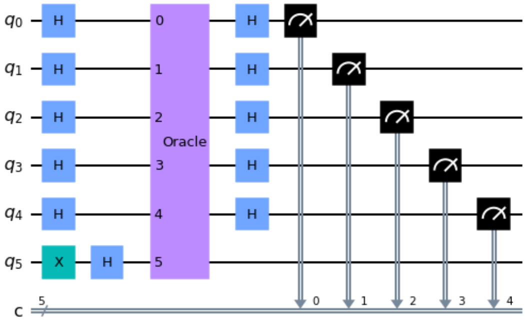
$|\widetilde{\psi_2}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$

$$|\psi_3\rangle = (H^{\otimes n})|\widetilde{\psi_2}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} H^{\otimes n} |x\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{xy} |y\rangle\right)$$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \left(\sum_{y \in \{0,1\}^n} (-1)^{f(x)} (-1)^{xy}\right) |y\rangle)$$

$$xy := x_0 y_0 \oplus x_1 y_1 \oplus \ldots x_{n-1} y_{n-1}$$



Cuarto paso: medimos los primeros n qubits.

¡Medimos! Testeamos $|0\rangle^{\otimes n}$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \Big(\sum_{y\in\{0,1\}^n} (-1)^{f(x)}(-1)^{xy}\Big)|y\rangle\Big)$$

La amplitud de probabilidad del $|0\rangle^{\otimes n}$ queda:

$$p_{|0\ldots0\rangle\langle0\ldots0|} = \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \right|^2$$

Si f es constante, $p_{|0\ldots0\rangle\langle0\ldots0|} = 1$.

Si f es balanceada, $p_{|0\ldots0\rangle\langle0\ldots0|} = 0$.

Si mido y obtengo $|0\ldots0\rangle\langle0\ldots0|$ era constante. Si obtengo cualquier otro resultado, era balanceada.

Algoritmo no determinista

- Hay 2^n inputs posibles (hay muchos). La solución clásica exacta es exponencial: $2^{N-1} + 1$ evaluaciones para estar seguros.
- En el caso no determinista, vamos realizando evaluaciones de inputs tomados al azar. Fijamos un número c de consultas (independiente del tamaño del problema)
  - Elegimos c inputs al azar
- Realizamos c consultas (evaluamos la función c veces)
- Si f es constante:
  - Obtenemos todos ceros o todos unos en las c consultas
- Si f es balanceada:
  - Si obtenemos algunos ceros y algunos unos en las consultas: deducimos que es balanceada
  - ¿Qué pasa si obtenemos todos resultados iguales, pero la f era balanceada?

Caso problemático

- El problema ocurre si f es balanceada pero:
  - Por mala suerte, obtenemos c ceros o c unos
  - Esto puede pasar ya que normalmente $c \ll 2^{n-1} + 1$
  - En este caso, si por observar todo igual, concluimos que la f era constante, la respuesta del algoritmo sería incorrecta
- ¿Cuál es la probabilidad de obtener una respuesta incorrecta si apostamos a que es constante en este escenario?

Supongamos que los c inputs dan cero, pero f es balanceada:

- Para el primer cero:
  - 2^{n-1} inputs con output cero
  - Probabilidad: $\frac{2^{n-1}}{2^n}$
- Para el segundo cero:
  - Quedan $2^{n-1}-1$ posibilidades
  - Probabilidad: $\frac{2^{n-1}-1}{2^n-1}$
- Para el tercer cero:
  - Probabilidad: $\frac{2^{n-1}-2}{2^n-2}$

...

- Para el c-ésimo cero:
  - Probabilidad: $\frac{2^{n-1}-(c-1)}{2^n-(c-1)}$
- La probabilidad de obtener c ceros consecutivos es:

$$\frac{2^{n-1}}{2^n} \cdot \frac{2^{n-1}-1}{2^n-1} \cdot \frac{2^{n-1}-2}{2^n-2} \cdots \frac{2^{n-1}-(c-1)}{2^n-(c-1)}$$

- Que puede escribirse compactamente como:

$$\prod_{k=0}^{c-1} \frac{2^{n-1}-k}{2^n-k}$$

- Simplificación de la expresión de probabilidad:

$$\frac{2^{n-1}}{2^n} \cdot \frac{2^{n-1}-1}{2^n-1} \cdots \frac{2^{n-1}-c}{2^n-c} \sim \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} = \frac{1}{2^c}$$

- Si hubiéramos obtenido todos unos (con función balanceada):
    - Probabilidad de error análoga: $\frac{1}{2^c}$
- Probabilidad de que salgan todos ceros o todos unos:

$$\frac{1}{2^c}(\text{para todos ceros}) + \frac{1}{2^c}(\text{para todos unos}) = \frac{1}{2^{c-1}}$$

- Complejidad del algoritmo:
    - $c = O(1)$ (constante)
    - Por lo tanto, ya no hay mucha ventaja en aplicar el algoritmo cuántico