Codificación Superdensa y Teleportación Cuántica

Vamos a ver los dos primeros protocolos de comunicación cuántica. Ambos son inherentemente cuánticos: no hay protocolos clásicos que se comporten como ellos. Se identificará a las dos partes como "Alice" y "Bob" como es usual en los protocolos de comunicación. Los protocolos requieren que Alice y Bob compartan inicialmente un par enredado de qubits en el *estado de Bell* o *par EPR*

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Tal estado puede haber sido creado cuando los qubits están juntos en un laboratorio y haberlos hecho interactuar para obtener el entanglement entre ellos. Después, Alice y Bob se llevan cada uno su qubit y se supone que no interactúan con el entorno de forma que continúan entangled.

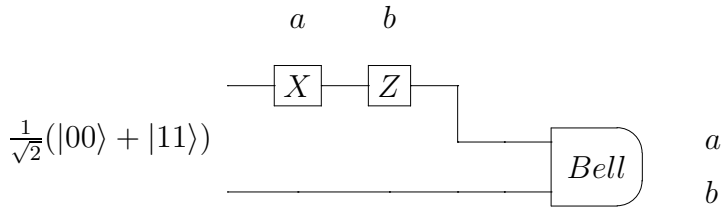
A. Codificación Superdensa

Supongamos que Alice quiere mandar a BOB dos bits clásicos de información. Como dijimos antes, ambos comparten el estado de Bell $|\beta_{00}\rangle$ y supongamos que Alice tiene el primer qubit y Bob el segundo. Alice aplica a su qubit una de las cuatro posibles compuertas de 1-qubit a su qubit de acuerdo a la siguiente tabla:

Para mandar	*Transformación*	
00	$I \otimes I$:	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \to \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) = \|\beta_{00}\rangle$
01	$X \otimes I$:	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \to \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle) = \|\beta_{01}\rangle$
10	$Z \otimes I$:	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \to \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle) = \|\beta_{10}\rangle$
11	$ZX \otimes I$:	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle) \to \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle) = \|\beta_{11}\rangle$

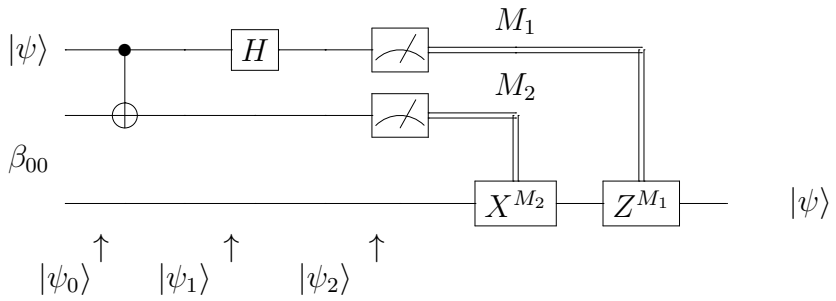
Verifique los resultados de arriba. Después de aplicar la compuerta apropiada, Alice manda su qubit a Bob. Ahora Bob puede realizar una medición del estado conjunto de dos qubits con respecto a la base de Bell. Esta medición ya fue descripta en la sección anterior.

La medición del estado de Bell permite a Bob ver qué estado de Bell tiene y determinar los dos bits clásicos que Alice le quería transmitir (a y b en la Figura).
El circuito correspondiente se muestra en la Figura:



B. Teleportación Cuántica

La teleportación cuántica es una técnica para transmitir estados cuánticos sin necesidad de un canal de comunicación cuántico. En la misma forma que para codificación superdensa, Alice y Bob comparten el par $|\beta_{00}\rangle$ desde algún tiempo previo. Supongamos que Alice quiere transmitir a Bob un qubit $|\psi\rangle$.
La idea es que Alice haga interactuar este qubit $|\psi\rangle$ con su mitad del par EPR y mida los dos qubits que tiene, obteniendo alguno de los cuatro resultados posibles: 00, 01, 10, 11. Ella envía esta información a Bob. Éste realiza una de cuatro operaciones sobre su mitad del par EPR y *recupera* el estado $|\psi\rangle$.
El circuito correspondiente se muestra en la Figura:



Las líneas de arriba son las de Alice y la de abajo es de Bob.

El qubit a ser teleportado es $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde α y β son amplitudes desconocidas. El estado de entrada es

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle|\beta_{00}\rangle \\ &= \tfrac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)], \end{aligned}$$

donde usamos la convención que los primeros qubits (empezando por la izquierda) son los de Alice y el tercero es el de Bob.

Despues que los qubits de Alice pasen por la compuerta CNOT se obtiene:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)].$$

Despues de la compuerta de Hadamard:

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)].$$

que reagrupando términos se convierte en

$$\begin{aligned} |\psi_2\rangle &= \tfrac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)\right. \\ &\quad \left. + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]. \end{aligned}$$

De acuerdo a esta expresión, la medición de los qubits de Alice determina el estado que tiene Bob:

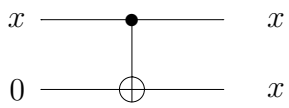
Alice	*Bob*
00	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle)$
10	$\alpha\|0\rangle - \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle)$

De forma que si Alice le transmite a Bob por un canal clásico los dos bits resultados de su medición, Bob hará las transformaciones correspondientes a su estado para obtener el $|\psi\rangle$ original. Si los bits de Alice son 00, Bob no hace nada porque ya tiene a $|\psi\rangle$. Si son 01 aplicará X. 10 aplicará Z y finalmente 11 aplicará XZ. Esto está reflejado en la figura con las compuertas X^{M_2} y Z^{M_1}.

Es posible transmitir información más rápido que la velocidad de la luz a través de la teleportación cuántica? Esto violaría la teoría de la relatividad. La necesidad de transmitir la información de la medida de los qubits de Alice por medio de un canal clásico necesariamente limitado a velocidades menores que la de la luz resuelve esta paradoja aparente.
También es importante señalar que no se realiza una *copia* o *clonado* del qubit original. Ésto no sucede porque si bien se *arma* el estado igual al original, éste termina en uno de los estados de la base computacional $|0\rangle$ o $|1\rangle$.

Copia de Qubits

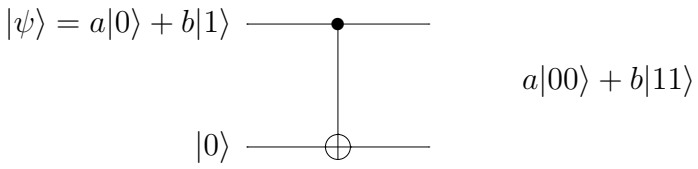
Clásicamente la copia de bits es sencilla de hacer. Se puede usar el circuito de la figura con una compuerta CNOT en la que se introduce un bit de entrada a copiar en un estado desconocido x y como *target* un bit igual a cero. La salida son dos bits iguales a x, de forma que se logró copiar el bit de entrada.



Supongamos que tratamos de hacer lo mismo con un qubit en el estado desconocido $|\psi\rangle = a|0\rangle + b|1\rangle$ usando de la misma manera que antes una compuerta CNOT. El estado input de los dos qubits será

$$[a|0\rangle + b|1\rangle]\,|0\rangle = a|00\rangle + b|10\rangle$$

y el circuito con la salida resultante será



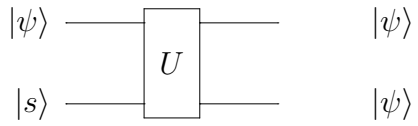
Se ha logrado copiar $|\psi\rangle$? Para eso se debería haber obtenido $|\psi\rangle|\psi\rangle$ que es:

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle$$

Vemos que a menos que $a = 0$ o $b = 0$ no se logró copiar el qubit de entrada. De hecho es *imposible* hacer una copia de un estado cuántico desconocido. Esta propiedad, que los qubits no pueden ser copiados, se conoce como el teorema de *no-clonado*.

Demostración del Teorema de No-Clonado

Supongamos que tenemos dos entradas al circuito de clonado de la siguiente forma



$|\psi\rangle$ es el estado a ser copiado y $|s\rangle$ es algún estado puro estandar. La transformación sería

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle|\psi\rangle.$$

Si se aplica a otro estado $|\varphi\rangle$ se tendrá

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle|\varphi\rangle.$$

Tomando el producto interno de estas dos ecuaciones se obtiene

$$(\langle\psi|\langle s|)U^\dagger U(|\varphi\rangle \otimes |s\rangle) = (\langle\psi|\varphi\rangle)^2$$

y usando que $U^\dagger = U^{-1}$, queda

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

Como $x = x^2$ tiene sólo dos soluciones, $x = 0$ y $x = 1$, $|\psi\rangle = |\varphi\rangle$ o $|\psi\rangle$ y $|\varphi\rangle$ son ortogonales. O sea que un dispositivo cuántico de clonado puede sólo clonar estados ortogonales entre sí y, por lo tanto, un dispositivo cuántico de clonado general es imposible, ya que por ejemplo no puede clonar los estados $|0\rangle$ y $(|0\rangle + |1\rangle)/\sqrt{2}$, dado que no son ortogonales.

Lo que hemos demostrado es que es imposible clonar estados cuánticos desconocidos con evoluciones unitarias. Se ha investigado otras variantes, tales como estados mixtos, evoluciones no-unitarias, pero el clonado es imposible de cualquier manera.

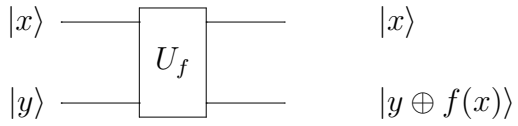
Algoritmos Cuánticos Introductorios

C. Kick-Back de fase

Consideremos ahora el efecto de una compuerta general de 2-qubits U_f que hace la transformación

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle,$$

donde $f(x)$ es una transformación arbitraria $f : \{0,1\} \to \{0,1\}$. El circuito correspondiente es



Fijemos ahora el bit target ($|y\rangle$) al estado $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\begin{aligned} U_f : |x\rangle\Big(|0\rangle - |1\rangle/\sqrt{2}\Big) \;&\to\; \Big(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\Big)/\sqrt{2} \\ &=\; \Big(|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\Big)/\sqrt{2} \\ &=\; |x\rangle\Big(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\Big)/\sqrt{2} \end{aligned}$$

Sabemos que $\oplus f(x)$ no tiene efecto sobre un bit si $f(x) = 0$ y cambia el estado del bit si $f(x) = 1$. Entonces

$$\begin{aligned} f(x) = 0 : \quad |0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle \;&=\; |0\rangle - |1\rangle \\ f(x) = 1 : \quad |0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle \;&=\; |1\rangle - |0\rangle \end{aligned}$$

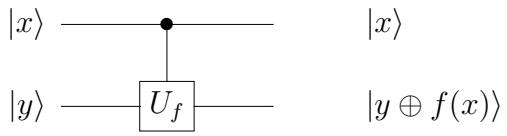
De forma que

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

y la acción de U_f resulta

$$U_f : |x\rangle\Big(|0\rangle - |1\rangle\Big)/\sqrt{2} \rightarrow (-1)^{f(x)}|x\rangle\Big(|0\rangle - |1\rangle\Big)/\sqrt{2}.$$

De forma que se puede hacer la equivalencia de U_f como un operador de 1 qubit $U_{f(x)}$ que transforma $|b\rangle \rightarrow |b \oplus f(x)\rangle$ actuando sobre el segundo qubit *controlado* por el estado $|x\rangle$ del primer registro como se muestra en la figura



D. El Algoritmo de Deutsch

El algoritmo de Deutsch es el primer algoritmo cuántico que se presenta porque es simple y fácil de entender y a la vez ilustra ideas claves de los algoritmos cuánticos como el *paralelismo* y la *interferencia* cuánticos.

El problema planteado es el siguiente. Supongamos que tenemos un circuito reversible que calcula una función de 1 bit desconocida $f : \{0, 1\} \rightarrow \{0, 1\}$ y tratamos este circuito como "caja negra" o "oráculo", lo que significa que lo podemos aplicar para calcular valores de $f(x)$ para distintos valores de x, pero no podemos acceder a las acciones internas del circuito para saber algo mas de la función $f(x)$. El problema es determinar $f(0) \oplus f(1)$. Si se obtiene que $f(0) \oplus f(1) = 0$, entonces podemos decir que $f(0) = f(1)$ (aunque no sepamos el valor) y f es "constante". Si, por el contrario, determinamos que $f(0) \oplus f(1) = 1$, sabemos que $f(0) \neq f(1)$ y se dice que la función es "balanceada".

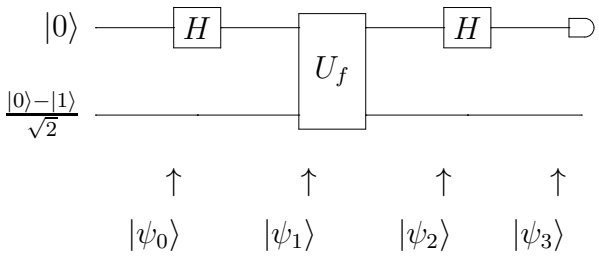
El Problema de Deutsch

Se tiene una "caja negra" para calcular una función desconocida $f : \{0, 1\} \rightarrow \{0, 1\}$.

Problema: Determinar $f(0) \oplus f(1)$ haciendo consultas por f.

Cuántas consultas son necesarias clásicamente para determinar $f(0) \oplus f(1)$? La respuesta es 2. Supongamos que la primer consulta es para determinar $f(0)$. Para determinar $f(0) \oplus f(1)$ necesitamos conocer $f(1)$ lo que obliga a la segunda consulta. El algoritmo

de Deutsch permite determinar $f(0) \oplus f(1)$ con *una sola consulta* al oráculo. El circuito correspondiente es



Vamos a analizar los estados en cada etapa del circuito.
El estado de entrada es

$$|\psi_0\rangle = |0\rangle\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big).$$

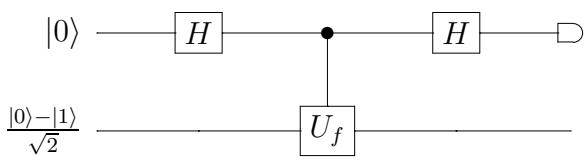
Despues de la primer compuerta de Hadamard aplicada al primer qubit

$$\begin{aligned} |\psi_1\rangle &= \Big(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\Big)\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) \\ &= \tfrac{1}{\sqrt{2}}|0\rangle\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) + \tfrac{1}{\sqrt{2}}|1\rangle\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big). \end{aligned}$$

La aplicación de U_f produce de acuerdo a lo visto en la sección anterior

$$\begin{aligned} |\psi_2\rangle &= \tfrac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) + \tfrac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) \\ &= \Big(\tfrac{-1^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}}\Big)\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) \\ &= (-1)^{f(0)}\Big(\tfrac{|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\Big)\Big(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) \end{aligned}$$

La última igualdad se debe a que $(-1)^{f(0)}(-1)^{f(1)} = (-1)^{f(0)\oplus f(1)}$.
También de acuerdo a la sección anterior se puede representar el circuito de la siguiente forma



Si f es una función constante ($f(0) \oplus f(1) = 0$), entonces resulta

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

y la compuerta final de Hadamard sobre el primer qubit transforma el estado en

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

Si f es una función balanceada ($f(0) \oplus f(1) = 1$), entonces resulta

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

y la compuerta final de Hadamard sobre el primer qubit transforma el estado en

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

O sea que si la función es constante se mide $|0\rangle$ y si es balanceada se mide $|1\rangle$.

E. El Algoritmo de Deutsch-Josza

El Algoritmo de Deutsch-Josza resuelve un problema que es una generalización del problema de Deutsch a funciones de n-bits. En este caso,

$$f : \{0,1\}^n \to \{0,1\}.$$

También sabemos que f es *constante* ($f(x)$ es la misma para todo x) o *balanceada* ($f(x) = 0$ para exactamente la mitad de los x y $f(x) = 1$ para la otra mitad). El problema es determinar si f es constante o balanceada haciendo consultas al circuito para f.
Con el algoritmo clásico, supongamos que hemos consultado el valor de $f(x)$ para la mitad de todos los x y que en todos los casos ha dado $f(x) = 0$. Todavía no podemos asegurar si es constante o balanceada porque puede ser que $f(x) = 0$ o $f(x) = 1$ para el resto. O

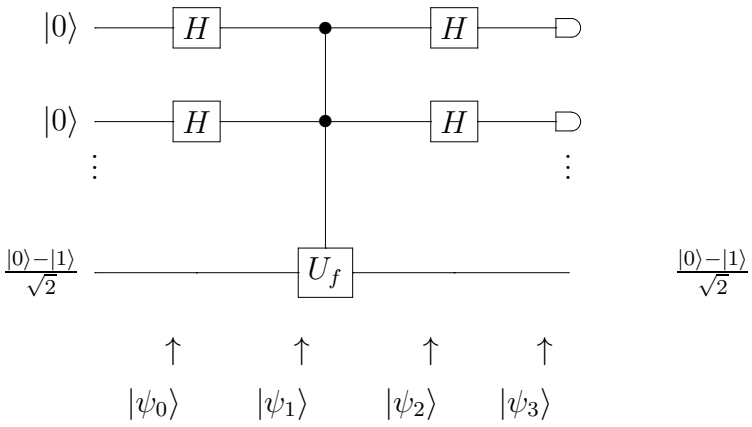
sea que no podemos decidir si es constante o balanceada hasta hacer $2^{n-1}+1$ consultas. El Algoritmo de Deutsch-Josza hace solamente una consulta a la versión cuántica del circuito para f.

Se define la operación cuántica

$$U_f : |\mathbf{x}\rangle|y\rangle \rightarrow |\mathbf{x}\rangle|y \oplus f(\mathbf{x})\rangle.$$

$\mathbf{x}$ indica una cadena de n-bits. Como antes U_f se toma como un operador de 1-qubit, pero ahora controlado por los qubits en el estado $|\mathbf{x}\rangle$.

El circuito para el algoritmo de Deutsch-Josza se muestra en la figura



Nótese la similaridad con el circuito del algoritmo de Deutsch. En lugar de una sola compuerta de Hadamard se tiene n compuertas de Hadamard en paralelo que se denota $H^{\otimes n}$. Se usa $|0^{\otimes n}\rangle$ o $|\mathbf{0}\rangle$ para el estado producto tensorial de n bits cada uno en $|0\rangle$. El estado inicial es

$$|\psi_0\rangle = |0\rangle^{\otimes n}\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big).$$

La acción de las n compuertas de Hadamard sobre $|0\rangle^{\otimes n}$ es

$$H^{\otimes n}|0\rangle^{\otimes n} = \Big(\frac{1}{\sqrt{2}}\Big)^n \underbrace{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}_{n}.$$

Desarrollando el producto tensorial:

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

El resultado es una superposición de todos los estados de la base de n-qubits todos con la misma amplitud $\frac{1}{\sqrt{2^n}}$. Entonces el estado posterior a la primer compuerta $H^{\otimes n}$ es

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

El estado despues de U_f es

$$\begin{aligned} |\psi_2\rangle &= \tfrac{1}{\sqrt{2^n}} U_f \Big(\textstyle\sum_{\mathbf{x}\in\{0,1\}} |\mathbf{x}\rangle \Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) \\ &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}} (-1)^{f(x)} |\mathbf{x}\rangle \Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big) \end{aligned}$$

donde hemos usado la equivalencia de la acción de U_f que vimos antes.

Ahora tenemos que ver la acción de la segunda compuerta de n-qubits de Hadamard sobre los estados de la base de n-qubits $|\mathbf{x}\rangle$.

El efecto de la compuerta Hadamard de 1-qubit sobre un estado de la base $|x\rangle$ puede ser escrito como

$$\begin{aligned} H|x\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \\ &= \tfrac{1}{\sqrt{2}} \textstyle\sum_{z\in\{0,1\}} (-1)^{xz}|z\rangle. \end{aligned}$$

Entonces se puede ver que la acción de la transformación de Hadamard sobre un estado de la base de n-qubits $|\mathbf{x}\rangle = |x_1\rangle|x_2\rangle \ldots |x_n\rangle$ es

$$\begin{aligned} H^{\otimes n}|\mathbf{x}\rangle &= H^{\otimes n}(|x_1\rangle|x_2\rangle \ldots |x_n\rangle) \\ &= H|x_1\rangle H|x_2\rangle \ldots H|x_n\rangle \\ &= \tfrac{1}{\sqrt{2}} \textstyle\sum_{z_1\in\{0,1\}} (-1)^{x_1 z_1}|z_1\rangle \ldots \tfrac{1}{\sqrt{2}} \sum_{z_n\in\{0,1\}} (-1)^{x_n z_n}|z_n\rangle \\ &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{z_1 z_2 \ldots z_n\in\{0,1\}} (-1)^{x_1 z_1 x_2 z_2 \ldots x_n z_n}|z_1\rangle|z_2\rangle \ldots |z_n\rangle. \end{aligned}$$

Esta expresión se puede poner

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

donde $\mathbf{x}.\mathbf{z}$ indica el producto interno modulo 2 de $\mathbf{x}$ y $\mathbf{z}$. El estado despues de la compuerta

final de n-qubits de Hadamard es

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

$$= \frac{1}{2^n}\sum_{\mathbf{z}\in\{0,1\}^n}\left(\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})+\mathbf{x}.\mathbf{z}}|\mathbf{z}\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).$$

Al final se realiza una medición de los n qubits de control en la base computacional. Consideremos la amplitud total de $|\mathbf{z}\rangle = |0\rangle^{\otimes n}$ en $|\psi_3\rangle$:

$$\frac{1}{2^n}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}.$$

Consideremos esta amplitud en los dos casos: f constante y f balanceada. Si es constante, la amplitud de $|0\rangle^{\otimes n}$ es $+1$ o -1 según el valor de $f(x)$. Así si f es constante la medición de los n qubits va a dar con *certeza* todos 0 (la cadena binaria $00\ldots0$). Por el otro lado, si f es balanceada, las contribuciones positivas y negativas de las amplitudes se cancelan y la amplitud de $|0\rangle^{\otimes n}$ es 0. De forma que en este caso se tiene la certeza de que *no se van a medir todos* 0.

Entonces la medición de los n qubits de control en la base computacional nos indica si f es constante o balanceada.

Es interesante señalar que aunque los algoritmos clásicos deterministas requerirían $2^{n-1}+1$ corridas en el peor de los casos (en el cuántico solamente 1), un algoritmo probabilístico clásico podría resolver el problema de Deutsch-Josza con probabilidad de error de como máximo $\frac{1}{3}$ en 2 corridas. La probabilidad de error puede ser reducida a menos que $\frac{1}{2^n}$ con $n+1$ corridas. Así, aunque hay un gap exponencial entre las complejidades clásica determinista y cuántica, el gap entre la probabilista clásica y la cuántica es constante en el caso de error constante y puede ser amplificado a un gap lineal para errores exponencialmente pequeños.