# Procesamiento Cuántico de Datos

Miguel Arizmendi, Gustavo Zabaleta

1 de diciembre de 2016

Sitio web: www3.fi.mdp.edu.ar/fes/ProcQ.html

# Codificación Superdensa y Teleportación Cuántica

# Codificación Superdensa

## Dos primeros protocolos de comunicación cuántica

- Inherentemente cuánticos.
- Se identificará a las dos partes como "Alice" y "Bob".
- 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.

# Codificación Superdensa

## Codificación Superdensa

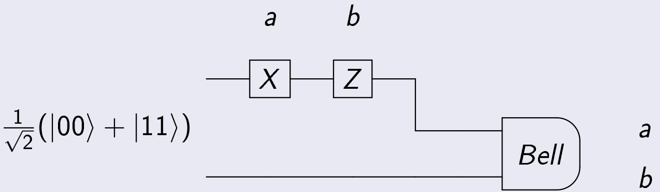
- Alice quiere mandar a BOB dos bits clásicos de información.
- Ambos comparten el estado de Bell $|\beta_{00}\rangle$
- Alice tiene el primer qubit y Bob el segundo.
- Alice aplica a su qubit una de las cuatro posibles compuertas de 1-qubit a su qubit, de acuerdo a:

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

# Codificación Superdensa

## Codificación Superdensa

- Después de aplicar la compuerta apropiada, Alice manda su qubit a Bob.
- Bob puede realizar una medición del estado conjunto de dos qubits con respecto a la base de Bell.
- Esto 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).



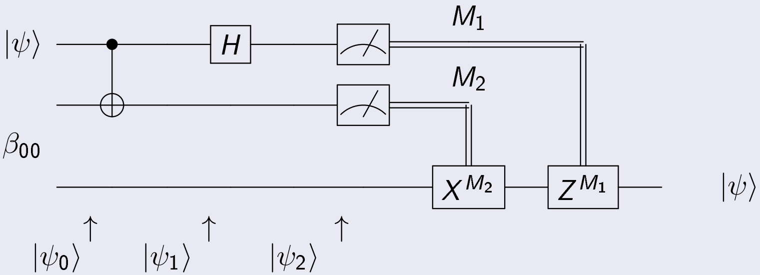
# Teleportación Cuántica

## Teleportación Cuántica

- Es una técnica para transmitir estados cuánticos sin necesidad de un canal de comunicación cuántico.
- Alice y Bob comparten el par $|\beta_{00}\rangle$ desde algún tiempo previo.
- Supongamos que Alice quiere transmitir a Bob un qubit $|\psi\rangle$.
  1. Alice hace interactuar $|\psi\rangle$ con su mitad del par EPR.
  2. Mide los dos qubits que tiene, obteniendo alguno de los cuatro resultados posibles: 00, 01, 10, 11.
  3. Ella envía esta información a Bob.
  4. Éste realiza una de cuatro operaciones sobre su mitad del par EPR y *recupera* el estado $|\psi\rangle$.

# Teleportación Cuántica

## Circuito Teleportación Cuántica




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

# Teleportación Cuántica

## Teleportación Cuántica paso a paso

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

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

    - Convención: Los primeros qubits (empezando por la izquierda) son los de Alice y el tercero es el de Bob.

# Teleportación Cuántica

## Teleportación Cuántica paso a paso

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

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

- Después 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

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

# Teleportación Cuántica

## Teleportación Cuántica paso a paso

- 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 | $\alpha\|1\rangle - \beta\|0\rangle)$ |

- 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.

# Teleportación Cuántica

## Teleportación Cuántica paso a paso

- 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 $XZ$.

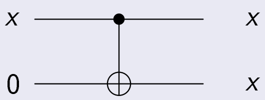
## ¿Se transmite información más rápido que la velocidad de la luz?

- Esto violaría la teoría de la relatividad.
- Alice necesita transmitir información por medio de un canal clásico necesariamente limitado a velocidades menores que la de la luz.

**También es importante señalar que no se realiza una *copia* o *clonado* del qubit original.**

# Copia de Qubits

## Caso clásico: Copia de bits




- $x$ es el bit de entrada a copiar, en un estado desconocido.
- *target* un bit igual a cero.
- La salida son dos bits iguales a $x$.
- Objetivo cumplido: Se copió $x$.

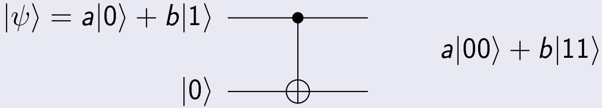
# Copia de Qubits

## Caso cuántico: Copia de bits

- El estado $|\psi\rangle = a|0\rangle + b|1\rangle$ del qubit de entrada a copiar.
- El estado input de los dos qubits será

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

- Circuito con la salida resultante:



# Copia de Qubits

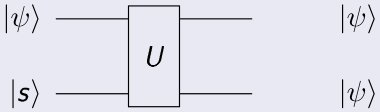
## ¿Se ha logrado copiar $|\psi\rangle$?

- No se obtuvo $|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle$.
- Salvo que $a = 0$ o $b = 0$ no se logró copiar el qubit de entrada.
- 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**.

# Copia de Qubits

## 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.

# Copia de Qubits

## Demostración del **Teorema de no-clonado**

- La transformación sería: $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle|\psi\rangle$.
- Si se aplica a otro estado $|\varphi\rangle \Rightarrow U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle|\varphi\rangle$.
- Tomando producto interno de estas dos ecuaciones

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

- 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.

# Copia de Qubits

## Teorema de no-clonado

- Un dispositivo cuántico de clonado puede sólo clonar estados ortogonales entre sí.
- Un dispositivo cuántico de clonado general es imposible.
- Ej: no puede clonar los estados $|0\rangle$ y $(|0\rangle + |1\rangle)/\sqrt{2}$, dado que no son ortogonales.

**Hemos demostrado que es imposible clonar estados cuánticos desconocidos con evoluciones unitarias.**

# Algoritmos Cuánticos Introductorios

# Algoritmos Cuánticos Introductorios

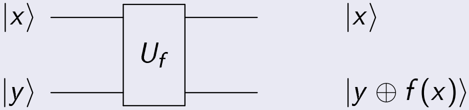
## Kick-Back de fase

- Consideremos 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



# Algoritmos Cuánticos Introductorios

## Kick-Back de fase

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

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

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

# Algoritmos Cuánticos Introductorios

## Kick-Back de fase

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

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

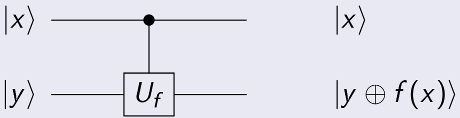
y la acción de $U_f$ resulta

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

# Algoritmos Cuánticos Introductorios

## Kick-Back de fase

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



# Algoritmos Cuánticos Introductorios

## Algoritmo de Deutsch

- Supongamos que tenemos un circuito reversible que calcula una función de 1 bit desconocida $f : \{0,1\} \rightarrow \{0,1\}$.
- tratamos este circuito como "caja negra" u "oráculo"
- Podemos 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 $f(x)$

Determinar $f(0) \oplus f(1)$

- Si $f(0) \oplus f(1) = 0 \rightarrow f(0) = f(1)$ y $f$ es "constante".
- Si $f(0) \oplus f(1) = 1 \rightarrow f(0) \neq f(1)$ y se dice que $f$ es "balanceada".

# Algoritmos Cuánticos Introductorios

## Problema de Deutsch

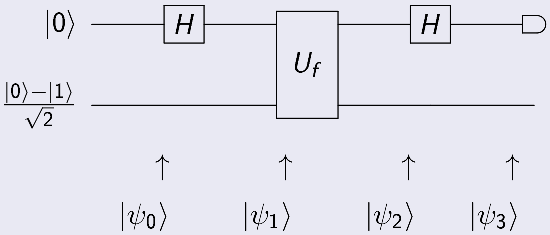
**Se tiene** una "caja negra" para calcular una función desconocida $f : \{0,1\} \to \{0,1\}$.

- Determinar $f(0) \oplus f(1)$ haciendo consultas por $f$.
- ¿Cuántas consultas son necesarias clásicamente para determinar $f(0) \oplus f(1)$? Rta: 2
- El algoritmo de Deutsch permite determinar $f(0) \oplus f(1)$ con *una sola consulta* al oráculo.

# Algoritmos Cuánticos Introductorios

## Problema de Deutsch

El circuito:



# Algoritmos Cuánticos Introductorios

## Estados en cada etapa del circuito de Deutsch

A la entrada:

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

Después de la primer compuerta de Hadamard aplicada al primer qubit

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

# Algoritmos Cuánticos Introductorios

## Estados en cada etapa del circuito de Deutsch

La aplicación de $U_f$ lleva a

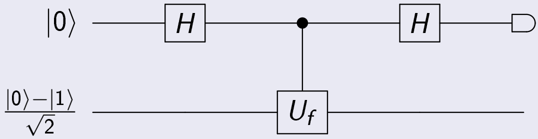
$$
\begin{aligned}
|\psi_2\rangle &= \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&= \left(\frac{-1^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)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

- La última igualdad se debe a que:

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

# Algoritmos Cuánticos Introductorios

## Otra forma de representar el circuito



# Algoritmos Cuánticos Introductorios

Concretamente:
Si $f$ :**cte.** $(f(0) \oplus f(1) = 0) \Rightarrow |\psi_2\rangle = (-1)^{f(0)} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$
y Hadamard sobre el primer qubit transforma el estado en:

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

Si $f$: **balanceada** $(f(0) \oplus f(1) = 1)$, entonces resulta

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

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

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

Entonces: Si $f$ : **cte.** se mide $|0\rangle$ y si $f$: **balanceada** se mide $|1\rangle$.

# Algoritmos Cuánticos Introductorios

## Problema de Deutsch-Josza

- Resuelve un problema que es una generalización del problema de Deutsch a funciones de n-bits.

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

- $f$ es *constante*: ($f(x)$ es la misma para todo $x$).
- $f$ es *balanceada*: ($f(x) = 0$ para exactamente la mitad de los $x$ y $f(x) = 1$ para la otra mitad).

Problema: Determinar si $f$ es constante o balanceada haciendo consultas al circuito para $f$.

# Algoritmos Cuánticos Introductorios

## Algoritmo Clásico Vs Algoritmo Cuántico

- 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 $f(x) = 0$.
- No podemos asegurar si es constante o balanceada porque puede ser que $f(x) = 0$ o $f(x) = 1$ para el resto.
- Por lo tanto debemos hacer $2^{n-1} + 1$ consultas para decidir si es constante o balanceada.

*El Algoritmo de Deutsch-Josza hace solamente* **una** *consulta a la versión cuántica del circuito para $f$.*

# Algoritmos Cuánticos Introductorios

## Problema de Deutsch-Josza

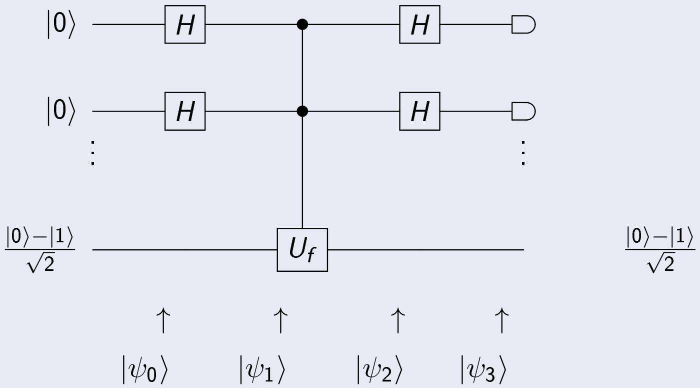
Se define la operación cuántica

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

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

# Algoritmos Cuánticos Introductorios

## Circuito para el algoritmo de Deutsch-Josza



# Algoritmos Cuánticos Introductorios

## Estados en cada etapa del circuito de Deutsch-Josza

- El estado inicial es

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

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

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

- Desarrollando el producto tensorial:

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

# Algoritmos Cuánticos Introductorios

## Estados en cada etapa del circuito de Deutsch-Josza

- el estado posterior a la primer compuerta $H^{\otimes n}$ es

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

- El estado después de $U_f$ es

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

# Algoritmos Cuánticos Introductorios

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

## Acción de la transformación de Hadamard sobre un estado de la base de $n$-qubits

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

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

# Algoritmos Cuánticos Introductorios

## Acción de la transformación de Hadamard sobre un estado de la base de $n$-qubits

- la transformación de Hadamard sobre un estado de la base de $n$-qubits $|\mathbf{x}\rangle = |x_1\rangle|x_2\rangle \dots |x_n\rangle$ es

$$H^{\otimes n}|\mathbf{x}\rangle = H^{\otimes n}(|x_1\rangle|x_2\rangle \dots |x_n\rangle) = H|x_1\rangle H|x_2\rangle \dots H|x_n\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |z_1\rangle \dots \frac{1}{\sqrt{2}} \sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} |z_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z_1 z_2 \dots z_n \in \{0,1\}^n} (-1)^{x_1 z_1 \oplus x_2 z_2 \oplus \dots \oplus x_n z_n} |z_1\rangle|z_2\rangle \dots |z_n\rangle.$$

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

# Algoritmos Cuánticos Introductorios

## Acción de la transformación de Hadamard sobre un estado de la base de $n$-qubits

La última xpresión se puede escribir

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

- $\mathbf{x}.\mathbf{z}$ indica el producto interno modulo 2 de $\mathbf{x}$ y $\mathbf{z}$.

# Algoritmos Cuánticos Introductorios

## Estados en cada etapa del circuito de Deutsch-Josza (sigue)

El estado después 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.

# Algoritmos Cuánticos Introductorios

## ¿Constante o Balanceada?

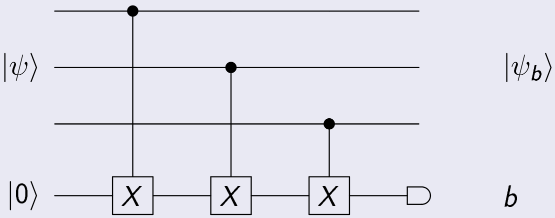
Consideremos la amplitud total de $|\mathbf{z}\rangle = |0\rangle^{\otimes n}$ en $|\psi_3\rangle$ :

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

- Si $f$ es constante, la amplitud de $|0\rangle^{\otimes n}$ es $+1$ o $-1$ según el valor de $f(x)$.
    - La medición de los $n$ qubits va a dar con *certeza* todos 0 (la cadena binaria $00\ldots0$).
- si $f$ es balanceada, las contribuciones positivas y negativas de las amplitudes se cancelan y la amplitud de $|0\rangle^{\otimes n}$ es 0.
    - 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.*

## Ejercicio 1: Circuito que calcula la paridad de estados de 3 qubits



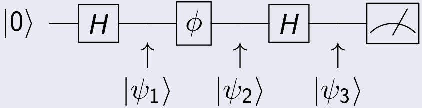

- Analice la salida del circuito para las distintas entradas posibles. Escriba en una tabla la salida de cada etapa:

Rta.: Ejercicio 1:

| $\|\psi_{in}\rangle\|0\rangle$ | $CNOT_1$ | $CNOT_2$ | $\|\psi_b\rangle$ | $b$ |
|---|---|---|---|---|
| 0000 | 0000 | 0000 | 000 | 0 |
| 0010 | 0010 | 0010 | 001 | 1 |
| 0100 | 0100 | 0101 | 010 | 1 |
| 0110 | 0110 | 0111 | 011 | 0 |
| 1000 | 1001 | 1001 | 100 | 1 |
| 1010 | 1011 | 1011 | 101 | 0 |
| 1100 | 1101 | 1100 | 110 | 0 |
| 1110 | 1111 | 1110 | 111 | 1 |

## Ejercicio 2: a) Interferómetro

Considere este modelo de un interferómetro de 1 qubit, donde el objetivo es estimar una fase desconocida $\phi$:

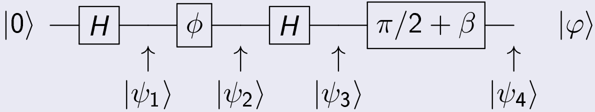



Considerando que la compuerta etiquetada $\phi$ mapea $|0\rangle \to |0\rangle$ y $|1\rangle \to e^{i\phi}|1\rangle$.

1. Escriba los estados $|\psi_1\rangle$, $|\psi_2\rangle$ y $|\psi_3\rangle$
2. ¿Cuál es la probabilidad de que el estado final sea 1?

## Ejercicio 2: Estado general de un qubit

b) Demuestre que, con diferencia de una fase global, el circuito de la figura genera el estado general de 1 qubit visto en la clase 2:



## Respuesta Ejercicio 2a)

1. $|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
   $|\psi_2\rangle = \frac{|0\rangle + e^{j\phi}|1\rangle}{\sqrt{2}}$
   $|\psi_3\rangle = \frac{1+e^{j\phi}}{2}|0\rangle + \frac{1-e^{j\phi}}{2}|1\rangle$
   Reacomodando términos queda:
   $|\psi_3\rangle = e^{j\phi/2}\left(cos(\phi/2)|0\rangle + e^{-j\pi/2}sin(\phi/2)|1\rangle\right)$

**Ejercicio 3: Compruebe que la compuerta de Toffoli, izquierda, tiene el circuito equivalente de la derecha, donde H es la compuerta de Hadamard, S es la compuerta fase, y T es la compuerta $\pi/8$**