Brevísima Introducción a la Computación Cuántica

Alejandro Díaz Caro[†], Julián Samborski Forlese[‡]

Departamento de Ciencias de la Computación - FCEIA - UNR

[†]diazcaro@fceia.unr.edu.ar, [‡]juliansf@gmail.com

Introducción

¿Qué es?

La computación cuántica es un **paradigma de computación** distinto al de la computación clásica.
Se basa en el uso de **qubits** en lugar de bits, y da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.
Una misma tarea puede tener **diferente complejidad** en computación clásica y en computación cuántica, lo que ha dado lugar a una gran expectación, ya que algunos problemas intratables pasan a ser tratables.

Algo habrán hecho...

- **1936** Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

Algo habrán hecho...

- **1936** Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

  Ley de Moore $\Rightarrow$ Dismunición en tamaño, mayor poder de cómputo. Sin embargo, los problemas que requieren recursos exponenciales siguen causando problemas.

Algo habrán hecho...

- **1936** Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

  Ley de Moore $\Rightarrow$ Dismunición en tamaño, mayor poder de cómputo. Sin embargo, los problemas que requieren recursos exponenciales siguen causando problemas.
- **1982** Richard Feynman sugiere que simular sistemas cuánticos necesariamente requiere recursos exponenciales. Sin embargo la naturaleza es capaz de simularlo de manera eficiente!

Algo habrán hecho...

- **1936** Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

  Ley de Moore $\Rightarrow$ Dismunición en tamaño, mayor poder de cómputo. Sin embargo, los problemas que requieren recursos exponenciales siguen causando problemas.
- **1982** Richard Feynman sugiere que simular sistemas cuánticos necesariamente requiere recursos exponenciales. Sin embargo la naturaleza es capaz de simularlo de manera eficiente!
- **1985** David Deustch describe el primer modelo para una Quantum Turing Machine basada en la utilización de datos y control cuánticos.

Algo habrán hecho...

- **1936** Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

  Ley de Moore $\Rightarrow$ Dismunición en tamaño, mayor poder de cómputo. Sin embargo, los problemas que requieren recursos exponenciales siguen causando problemas.
- **1982** Richard Feynman sugiere que simular sistemas cuánticos necesariamente requiere recursos exponenciales. Sin embargo la naturaleza es capaz de simularlo de manera eficiente!
- **1985** David Deustch describe el primer modelo para una Quantum Turing Machine basada en la utilización de datos y control cuánticos.
- **1993** Charles Bennet y otros cieníficos de IBM diseñaron el experimento de Teleportación.

Algo habrán hecho... (cont.)

- **1994** Peter Shor describe un algoritmo cuántico para factorizar números que es exponencialmente más rápido que cualquier algoritmo clásico conocido. El potencial de ese algoritmo atrajo mucha inversión de entes estatales y privados.

Algo habrán hecho... (cont.)

- **1994** Peter Shor describe un algoritmo cuántico para factorizar números que es exponencialmente más rápido que cualquier algoritmo clásico conocido. El potencial de ese algoritmo atrajo mucha inversión de entes estatales y privados.
- **1998** Isaac Chuang dirige el grupo de Berkeley que desarrolla la primera computadora cuántica de 1 qubit.

Algo habrán hecho... (cont.)

- **1994** Peter Shor describe un algoritmo cuántico para factorizar números que es exponencialmente más rápido que cualquier algoritmo clásico conocido. El potencial de ese algoritmo atrajo mucha inversión de entes estatales y privados.
- **1998** Isaac Chuang dirige el grupo de Berkeley que desarrolla la primera computadora cuántica de 1 qubit.
- **2001** Un grupo de IBM desarrolla una computadora cuántica capaz de controlar 7 qubits, con ella prueban el algoritmo de Shor factorizando el número 15.

Algo habrán hecho... (cont.)

- **1994** Peter Shor describe un algoritmo cuántico para factorizar números que es exponencialmente más rápido que cualquier algoritmo clásico conocido. El potencial de ese algoritmo atrajo mucha inversión de entes estatales y privados.
- **1998** Isaac Chuang dirige el grupo de Berkeley que desarrolla la primera computadora cuántica de 1 qubit.
- **2001** Un grupo de IBM desarrolla una computadora cuántica capaz de controlar 7 qubits, con ella prueban el algoritmo de Shor factorizando el número 15.
- **Diciembre de 2005** Rainer Blatt y su grupo de Innsbruck realizan una computadora cuántica de 8 qubits (1 qubyte) y Daniel Stick y su grupo de Michigan logran el primer chip capaz de controlar un qubit.

Algunos conceptos

Unidad mínima de información clásica: **BIT**.

Algunos conceptos

Unidad mínima de información clásica: **BIT**.

Unidad mínima de información cuántica: **QuBIT**.

Algunos conceptos

Unidad mínima de información clásica: **BIT**.

Unidad mínima de información cuántica: **QuBIT**.

Un qubit puede existir como 0, como 1 o como una **superposición** de 0 y 1. Esto permite que se puedan realizar cómputos sobre ambos valores a la vez.

Algunos conceptos

Unidad mínima de información clásica: **BIT**.

Unidad mínima de información cuántica: **QuBIT**.

Un qubit puede existir como 0, como 1 o como una **superposición** de 0 y 1. Esto permite que se puedan realizar cómputos sobre ambos valores a la vez.

Pensemos ésto: con una computadora clásica que manipule tan sólo 500 bits poco podría hacerse, pero para igualar a una computadora cuántica que manipule 500 qubits necesitaríamos manipular 2^{500} bits!

Algunos conceptos

Unidad mínima de información clásica: **BIT**.

Unidad mínima de información cuántica: **QuBIT**.

Un qubit puede existir como 0, como 1 o como una **superposición** de 0 y 1. Esto permite que se puedan realizar cómputos sobre ambos valores a la vez.

Pensemos ésto: con una computadora clásica que manipule tan sólo 500 bits poco podría hacerse, pero para igualar a una computadora cuántica que manipule 500 qubits necesitaríamos manipular 2^{500} bits!

$$2^{500} \simeq 10000000000000000000000000000000000000000000000000$$

$$00000000000000000000000000000000000000000000000000$$

$$00000000000000000000000000000000000000000000000000$$

¿Cómo se piensa cuánticamente?

Los algoritmos cuánticos requieren pensar en términos de superposición, lo cual trae aparejado un cambio de concepto para los programadores actuales.

¿Cómo se piensa cuánticamente?

Los algoritmos cuánticos requieren pensar en términos de superposición, lo cual trae aparejado un cambio de concepto para los programadores actuales.

Veamos un ejemplo concreto:
Problema: Encontrar un camino a través de un laberinto.

¿Cómo se piensa cuánticamente?

Los algoritmos cuánticos requieren pensar en términos de superposición, lo cual trae aparejado un cambio de concepto para los programadores actuales.

Veamos un ejemplo concreto:
Problema: Encontrar un camino a través de un laberinto.

Solución Clásica: Regla de la mano derecha. En cada bifurcación, siempre se tomará el camino hacia la derecha. Este método no garantiza encontrar el camino más corto pero si la salida.

¿Cómo se piensa cuánticamente?

Los algoritmos cuánticos requieren pensar en términos de superposición, lo cual trae aparejado un cambio de concepto para los programadores actuales.

Veamos un ejemplo concreto:
Problema: Encontrar un camino a través de un laberinto.

Solución Clásica: Regla de la mano derecha. En cada bifurcación, siempre se tomará el camino hacia la derecha. Este método no garantiza encontrar el camino más corto pero si la salida.

Solución Cuántica: Tomamos todos los caminos a la vez y, ni bien se encuentre una solución, vemos cuál ha sido el camino que se ha tomado. Esto garantiza no sólo que encuntramos la salida, sino que además, es la más corta.

Algoritmos Cuánticos

Actualmente existen tres grandes divisiones en el área de los algoritmos cuánticos que pueden ser caracterizados como:

Algoritmos Cuánticos

Actualmente existen tres grandes divisiones en el área de los algoritmos cuánticos que pueden ser caracterizados como:

- El problema del subgrupo escondido, que incluye al algoritmo de **Shor** como caso particular.

Algoritmos Cuánticos

Actualmente existen tres grandes divisiones en el área de los algoritmos cuánticos que pueden ser caracterizados como:

- El problema del subgrupo escondido, que incluye al algoritmo de **Shor** como caso particular.

- El Problemas de búsqueda y optimización que incluye el algoritmos de **Groover**.

Algoritmos Cuánticos

Actualmente existen tres grandes divisiones en el área de los algoritmos cuánticos que pueden ser caracterizados como:

- El problema del subgrupo escondido, que incluye al algoritmo de **Shor** como caso particular.

- El Problemas de búsqueda y optimización que incluye el algoritmos de **Groover**.

- Algoritmos basados en caminos aleatorios cuánticos.

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

- Algoritmo de búsqueda de **Groover** ($O(log_2 n)$).

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

- Algoritmo de búsqueda de **Groover** ($O(log_2 n)$).
- Algoritmo de **Shor** ($O((log_2 n)^3)$)

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

- Algoritmo de búsqueda de **Groover** ($O(log_2 n)$).
- Algoritmo de **Shor** ($O((log_2 n)^3)$)
- Algoritmo de **Kitaev** que sirve para calcular el orden de un grupo.

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

- Algoritmo de búsqueda de **Groover** ($O(log_2 n)$).
- Algoritmo de **Shor** ($O((log_2 n)^3)$)
- Algoritmo de **Kitaev** que sirve para calcular el orden de un grupo.
- Algoritmo de **Watrous** para calcular el orden de grupos solubles.

Algoritmos Cuánticos (cont.)

Los algoritmos cuánticos que actualmente más importancia tienes son:

- Algoritmo de búsqueda de **Groover** ($O(log_2 n)$).
- Algoritmo de **Shor** ($O((log_2 n)^3)$)
- Algoritmo de **Kitaev** que sirve para calcular el orden de un grupo.
- Algoritmo de **Watrous** para calcular el orden de grupos solubles.
- Descomposición de **Grupos Finitos Abelianos**.

Implementaciones???

Se están probando varias formas para lograr controlar qubits:

- Heteropolymers.
- Ion Traps.
- Cavidades Cuánticas Electrodinámicas.
- Resonancia Magnética Nuclear.
- Quantum Dots.
- Kane Computer (MNR).
- Josephson Junctions.
- Topological Quantum Computer

Lenguajes Cuánticos

- **QCL** (Quantum Computation Language, inspirado en C) [Omer 1998]
- **QPL** (Quantum Programming Language, control clásico y datos cuánticos) [Selinger 2004]
- **QML** (Quantum ML) [Altenkirch and Grattage 2005]
- **QHaskell** [Vizzotto and Da Rocha Costa 2006]

Qubits

Un qubit

Un qubit es un vector de la forma $\binom{\alpha}{\beta}$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$.

Un qubit

Un qubit es un vector de la forma $\binom{\alpha}{\beta}$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$.

Se considera una base del espacio de qubits, por ejemplo:

$$\left\{ \binom{1}{0}, \binom{0}{1} \right\}$$

Un qubit

Un qubit es un vector de la forma $\binom{\alpha}{\beta}$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$.

Se considera una base del espacio de qubits, por ejemplo:

$$\left\{ \binom{1}{0}, \binom{0}{1} \right\}$$

entonces un qubit tendrá la forma

$$\alpha \binom{1}{0} + \beta \binom{0}{1}$$

Un qubit

Un qubit es un vector de la forma $\binom{\alpha}{\beta}$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1$.
Se considera una base del espacio de qubits, por ejemplo:

$$\left\{ \binom{1}{0}, \binom{0}{1} \right\}$$

entonces un qubit tendrá la forma

$$\alpha \binom{1}{0} + \beta \binom{0}{1}$$

Llamaremos $|0\rangle$ al vector $\binom{1}{0}$ y $|1\rangle$ al vector $\binom{0}{1}$, así, a cualquier qubit $|\psi\rangle$ lo escribiremos como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle)$$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Compuertas Cuánticas para 1 qubit

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Compuertas Cuánticas para 1 qubit (cont.)

En los qubits de la base canónica vemos que

$$X|0\rangle = |1\rangle, \qquad X|1\rangle = |0\rangle$$

Por lo cual, la compuerta X es comunmente llamada *compuerta NOT*.

Compuertas Cuánticas para 1 qubit (cont.)

En los qubits de la base canónica vemos que

$$X|0\rangle = |1\rangle\,, \qquad X|1\rangle = |0\rangle$$

Por lo cual, la compuerta X es comunmente llamada *compuerta NOT*.

En general, la aplicación de una compuerta cuántica a un qubit se puede ver de la siguiente manera:

$$U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$$

Por lo cual, con sólo describir de qué manera actúa en una base, ya habremos descripto la compuerta completamente.

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

$$H|1\rangle$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

Otro ejemplo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Veamos cómo actúa sobre la base $\{|0\rangle, |1\rangle\}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

a este vector lo llamaremos $|+\rangle$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

a este vector lo llamaremos $|-\rangle$

Otro ejemplo (cont.)

Como podemos ver

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

y

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

son ortogonales, por lo tanto forman base:

$$B = \{|+\rangle, |-\rangle\}$$

Medición

Otros operadores muy importantes son los “operadores medición”, los cuales actúan de la siguiente manera:

Medición

Otros operadores muy importantes son los “operadores medición”, los cuales actúan de la siguiente manera:

Sea la base $B = \{|x\rangle, |y\rangle\}$, entonces

$$M_B\left(\alpha|x\rangle + \beta|y\rangle\right)$$

Medición

Otros operadores muy importantes son los “operadores medición”, los cuales actúan de la siguiente manera:

Sea la base $B = \{|x\rangle, |y\rangle\}$, entonces

$$M_B(\alpha|x\rangle + \beta|y\rangle) = \begin{cases} |x\rangle & \text{con probabilidad } |\alpha|^2 \\ |y\rangle & \text{con probabilidad } |\beta|^2 \end{cases}$$

Dos qubits

Para extender este sistema a 2 qubits haremos un “producto tensorial” entre las bases de cada sistema de 1 qubit.

Dos qubits

Para extender este sistema a 2 qubits haremos un “producto tensorial” entre las bases de cada sistema de 1 qubit.

Qué es un Producto Tensorial?

Dos qubits

Para extender este sistema a 2 qubits haremos un “producto tensorial” entre las bases de cada sistema de 1 qubit.

Qué es un Producto Tensorial?

“Qué es” es una pregunta demasiado grande para esta presentación... digamos simplemente cómo calcularlo

Dos qubits (cont.)

Producto tensorial entre matrices

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \otimes B$$

Dos qubits (cont.)

Producto tensorial entre matrices

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

Dos qubits (cont.)

Producto tensorial entre matrices

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

Producto tensorial entre vectores: ídem matrices

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \otimes w = \begin{pmatrix} v_1.w \\ v_2.w \\ \vdots \\ v_n.w \end{pmatrix}$$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.

Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $B_1 = \{|+\rangle, |-\rangle\}$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.
Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $B_1 = \{|+\rangle, |-\rangle\}$
entonces:

$$B_1 \otimes B_2 = \{|0\rangle \otimes |+\rangle, |0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle\}$$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.
Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $\quad B_1 = \{|+\rangle, |-\rangle\}$
entonces:

$$B_1 \otimes B_2 = \{|0\rangle \otimes |+\rangle, |0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle\}$$

Para simplificar, $|x\rangle \otimes |y\rangle$ lo notamos $|xy\rangle$.
O sea:

$$B_1 \otimes B_2 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.
Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $\quad B_1 = \{|+\rangle, |-\rangle\}$
entonces:

$$B_1 \otimes B_2 = \{|0\rangle \otimes |+\rangle, |0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle\}$$

Para simplificar, $|x\rangle \otimes |y\rangle$ lo notamos $|xy\rangle$.
O sea:

$$B_1 \otimes B_2 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$$

Otro ejemplo: $B_1 = B_2 = \{|0\rangle, |1\rangle\}$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.
Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $B_1 = \{|+\rangle, |-\rangle\}$
entonces:

$$B_1 \otimes B_2 = \{|0\rangle \otimes |+\rangle, |0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle\}$$

Para simplificar, $|x\rangle \otimes |y\rangle$ lo notamos $|xy\rangle$.
O sea:

$$B_1 \otimes B_2 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$$

Otro ejemplo: $B_1 = B_2 = \{|0\rangle, |1\rangle\}$

$$B_1 \otimes B_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Dos qubits (cont.)

Producto tensorial entre bases: Es el producto tensorial entre todos los vectores de una base con los de la otra.
Ejemplo: $B_1 = \{|0\rangle, |1\rangle\}$ $B_1 = \{|+\rangle, |-\rangle\}$
entonces:

$$B_1 \otimes B_2 = \{|0\rangle \otimes |+\rangle, |0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle\}$$

Para simplificar, $|x\rangle \otimes |y\rangle$ lo notamos $|xy\rangle$.
O sea:

$$B_1 \otimes B_2 = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle\}$$

Otro ejemplo: $B_1 = B_2 = \{|0\rangle, |1\rangle\}$

$$B_1 \otimes B_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Entonces podemos expresar un 2-qubit con respecto a esta última base así:

$$|\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |01\rangle + \alpha_3 |10\rangle + \alpha_4 |11\rangle$$

donde $\sum_{i=1}^{4} |\alpha_i|^2 = 1$

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle + |1\rangle)\right]$$

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle + |1\rangle)\right]$$

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

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle + |1\rangle)\right]$$

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

$$= |+\rangle \otimes |+\rangle = |++\rangle$$

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle + |1\rangle)\right]$$

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

$$= |+\rangle \otimes |+\rangle = |++\rangle$$

si aquí medimos el primer qubit con $M_{\{|0\rangle,|1\rangle\}}$ quedará:

Dos qubits (cont.)

Un ejemplo más:

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle + |1\rangle)\right]$$

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

$$= |+\rangle \otimes |+\rangle = |++\rangle$$

si aquí medimos el primer qubit con $M_{\{|0\rangle,|1\rangle\}}$ quedará:

$|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ con probabilidad $\frac{1}{2}$

y

$|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ con probabilidad $\frac{1}{2}$

Enredo cuántico (Entanglement)

No siempre podremos expresar un 2-qubit como producto tensorial de dos 1-qubit.

Enredo cuántico (Entanglement)

No siempre podremos expresar un 2-qubit como producto tensorial de dos 1-qubit.
Ejemplo: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

Enredo cuántico (Entanglement)

No siempre podremos expresar un 2-qubit como producto tensorial de dos 1-qubit.
Ejemplo: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
En este caso, al realizar una medición sobre el primer qubit con $M_{\{|0\rangle,|1\rangle\}}$ vemos que obtenemos:

$$|00\rangle \qquad \text{ó} \qquad |11\rangle$$

O sea, al medir el primer qubit, también obtenemos el segundo.

Enredo cuántico (Entanglement)

No siempre podremos expresar un 2-qubit como producto tensorial de dos 1-qubit.
Ejemplo: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
En este caso, al realizar una medición sobre el primer qubit con $M_{\{|0\rangle,|1\rangle\}}$ vemos que obtenemos:

$$|00\rangle \qquad \text{ó} \qquad |11\rangle$$

O sea, al medir el primer qubit, también obtenemos el segundo.
A esta propiedad se la llama “enredo cuántico” (entanglement) y se dice que estos dos qubits están “enredados” (entangled).

Paralelismo

Consideremos una función $f : \{0,1\} \rightarrow \{0,1\}$.

Paralelismo

Consideremos una función $f : \{0,1\} \to \{0,1\}$.

y una compuerta cuántica U_f tal que

$$U_f \left|x, y\right\rangle = \left|x, y \oplus f(x)\right\rangle$$

donde $\oplus$ simboliza la suma módulo 2

Paralelismo

Consideremos una función $f : \{0,1\} \to \{0,1\}$.

y una compuerta cuántica U_f tal que

$$U_f \left|x, y\right\rangle = \left|x, y \oplus f(x)\right\rangle$$

donde $\oplus$ simboliza la suma módulo 2
Por la definición anterior tenemos que

$$U_f \left|x, 0\right\rangle = \left|x, f(x)\right\rangle$$

Paralelismo

Consideremos una función $f : \{0,1\} \to \{0,1\}$.

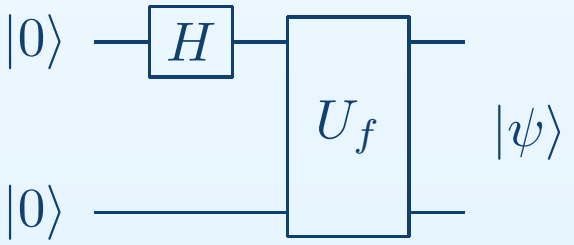
y una compuerta cuántica U_f tal que

$$U_f \left|x, y\right\rangle = \left|x, y \oplus f(x)\right\rangle$$

donde $\oplus$ simboliza la suma módulo 2
Por la definición anterior tenemos que

$$U_f \left|x, 0\right\rangle = \left|x, f(x)\right\rangle$$

Ahora consideremos el siguiente circuito



Paralelismo (cont.)

Veamos

$$|00\rangle$$

Paralelismo (cont.)

Veamos

$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$$

Paralelismo (cont.)

Veamos

$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Paralelismo (cont.)

Veamos

$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$\overset{U_f}{\longrightarrow} \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

Paralelismo (cont.)

Veamos

$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$\overset{U_f}{\longrightarrow} \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

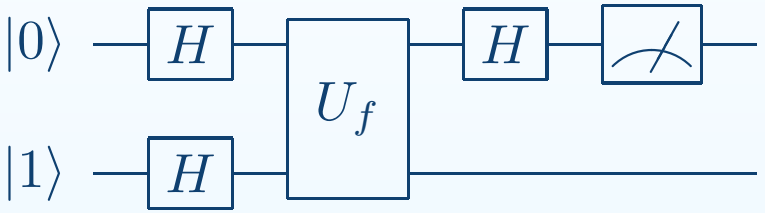
La salida de este circuito nos da un estado que es superposición de todos los resultados posibles de la aplicación de la función f. En principio esta no sería una idea muy práctica, ya que no podemos saber un valor particular de f.

Algoritmo de Deutsch

El objetivo de este algoritmo es saber si una función es constante.

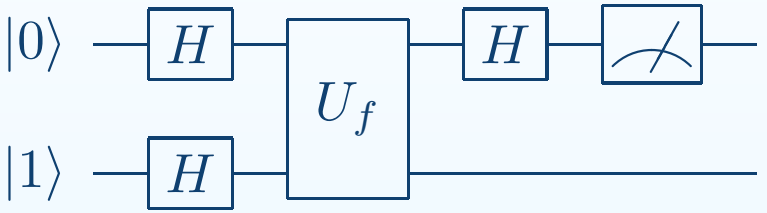
Algoritmo de Deutsch

El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



Algoritmo de Deutsch

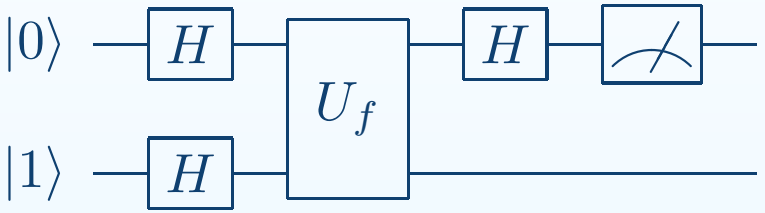
El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



$|01\rangle$

Algoritmo de Deutsch

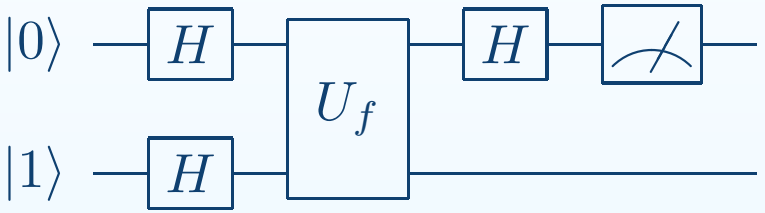
El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



$$|01\rangle \overset{H(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Algoritmo de Deutsch

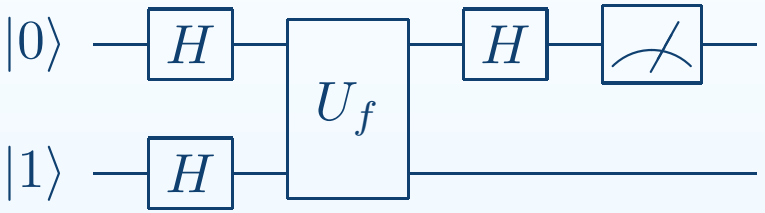
El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



$$|01\rangle \overset{H(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Algoritmo de Deutsch

El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



$$|01\rangle \overset{H(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

El siguiente paso es aplicar la compuerta U_f. Veamos qué sucede con cada una de las posibilidades

Algoritmo de Deutsch (cont.)

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

Algoritmo de Deutsch (cont.)

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

$$U_f |+, 0\rangle$$

$$=$$

Algoritmo de Deutsch (cont.)

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

$$U_f |+, 0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$=$

Algoritmo de Deutsch (cont.)

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

$$U_f |+, 0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$U_f |+, 1\rangle$

$=$

Algoritmo de Deutsch (cont.)

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

$$U_f |+,0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$$U_f |+,1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

$=$

Algoritmo de Deutsch (cont.)

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

$$U_f |+,0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$$U_f |+,1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

por lo tanto

$$U_f |+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$=$$

Algoritmo de Deutsch (cont.)

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

$$U_f |+,0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$$U_f |+,1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

por lo tanto

$$U_f |+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} U_f(|+,0\rangle - |+,1\rangle)$$

$$=$$

Algoritmo de Deutsch (cont.)

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

$$U_f |+,0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$$U_f |+,1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

por lo tanto

$$U_f |+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} U_f(|+,0\rangle - |+,1\rangle)$$

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

Algoritmo de Deutsch (cont.)

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

$$U_f |+,0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$$U_f |+,1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

por lo tanto

$$U_f |+\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} U_f(|+,0\rangle - |+,1\rangle)$$

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

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

Algoritmo de Deutsch (cont.)

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

Algoritmo de Deutsch (cont.)

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

$$= \frac{1}{2}\left(|0, f(0)\rangle + |1, f(1)\rangle - |0, 1 \oplus f(0)\rangle - |1, 1 \oplus f(1)\rangle\right)$$

Algoritmo de Deutsch (cont.)

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

$$= \frac{1}{2}\left(|0, f(0)\rangle + |1, f(1)\rangle - |0, 1 \oplus f(0)\rangle - |1, 1 \oplus f(1)\rangle\right)$$

Entonces, si $f(0) \neq f(1)$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)$$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|--\rangle$$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|--\rangle$$

y si $f(0)=f(1)$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|--\rangle$$

y si $f(0)=f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|10\rangle-|01\rangle-|11\rangle\right)$$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|--\rangle$$

y si $f(0)=f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|10\rangle-|01\rangle-|11\rangle\right)=\pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Algoritmo de Deutsch (cont.)

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

$$=\frac{1}{2}\left(|0,f(0)\rangle+|1,f(1)\rangle-|0,1\oplus f(0)\rangle-|1,1\oplus f(1)\rangle\right)$$

Entonces, si $f(0)\neq f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|11\rangle-|01\rangle-|10\rangle\right)=\pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|--\rangle$$

y si $f(0)=f(1)$

$$=\pm\frac{1}{2}\left(|00\rangle+|10\rangle-|01\rangle-|11\rangle\right)=\pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$=\pm|+-\rangle$$

Algoritmo de Deutsch (cont.)

Resumiendo:

$$\begin{cases} \pm|--\rangle & \text{si } f(0) \neq f(1) \\ \pm|+-\rangle & \text{si } f(0) = f(1) \end{cases}$$

Algoritmo de Deutsch (cont.)

Resumiendo:

$$\begin{cases} \pm|--\rangle & \text{si } f(0) \neq f(1) \\ \pm|+-\rangle & \text{si } f(0) = f(1) \end{cases}$$

Haciendo una medición con $M_{\{|+\rangle,|-\rangle\}}$ sobre el primer qubit podemos distinguir en cuál de los dos casos estamos.

Algoritmo de Deutsch (cont.)

Resumiendo:

$$\begin{cases} \pm|--\rangle & \text{si } f(0) \neq f(1) \\ \pm|+-\rangle & \text{si } f(0) = f(1) \end{cases}$$

Haciendo una medición con $M_{\{|+\rangle,|-\rangle\}}$ sobre el primer qubit podemos distinguir en cuál de los dos casos estamos.

En éste algoritmo no se puede apreciar del todo la ganancia, pero si la idea de paralelismo. Aquí tengo un orden de complejidad $O(3)$, al igual que el algoritmo clásico equivalente. La diferencia está en que la generalización de éste algoritmo a funciones de $N \to N$ (algoritmo de Deutsch-Jotza) sigue manteniendo el $O(3)$.

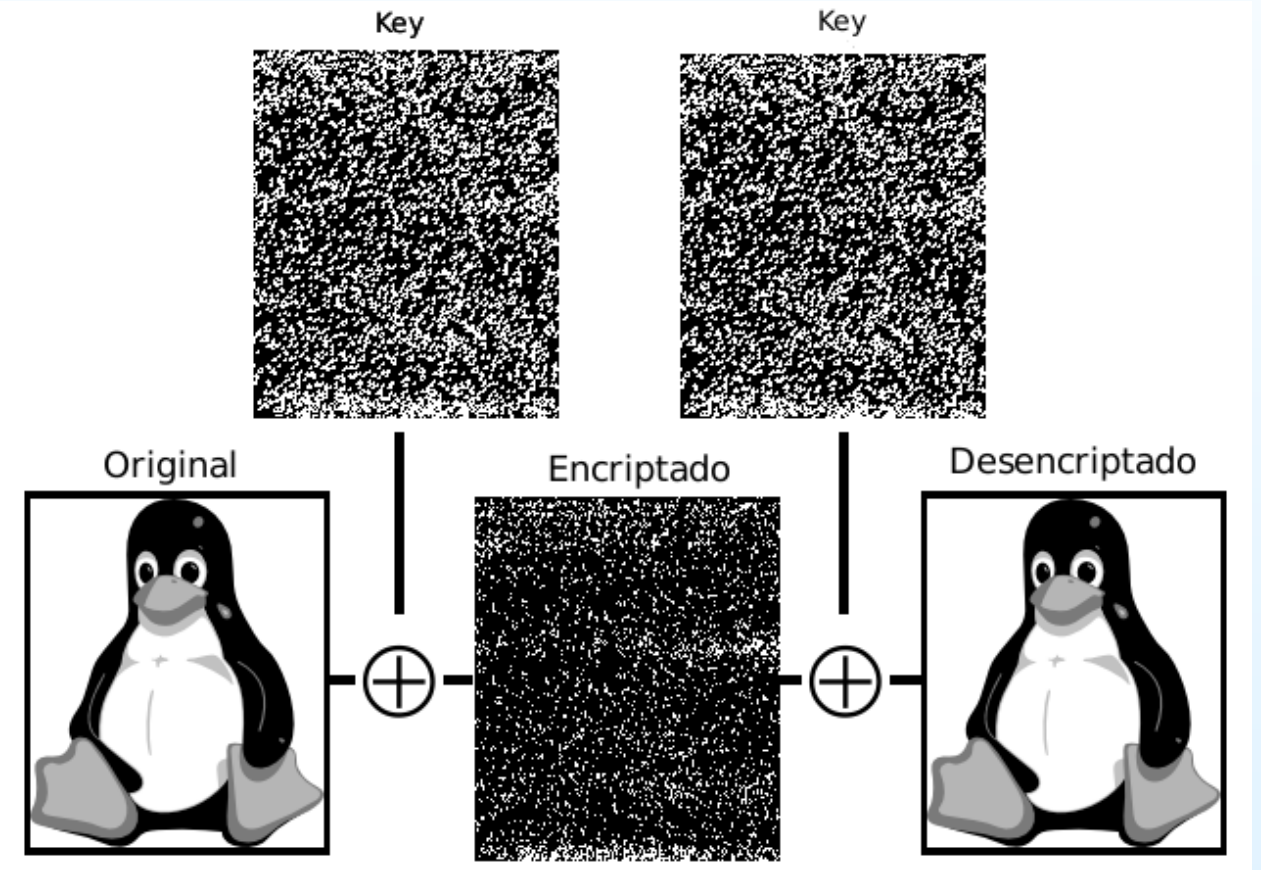
Algo de Criptografía

One Time Pad

Este es un méodo de criptografía **clásica** que consiste en compartir una secuencia de bits (clave) del largo del mensaje a transmitir y aplicar la operación (reversible) XOR para cifrar y decifrar.

One Time Pad

Este es un méodo de criptografía **clásica** que consiste en compartir una secuencia de bits (clave) del largo del mensaje a transmitir y aplicar la operación (reversible) XOR para cifrar y decifrar.



QKD-BB84

QKD-BB84

QKD = Quantum Key Distribution

QKD-BB84

QKD = Quantum Key Distribution
BB84 = Bennet, Brassard, 1984

QKD-BB84

QKD = Quantum Key Distribution
BB84 = Bennet, Brassard, 1984

- BB84 fue el primer protocolo 100 % seguro de distribución de claves.
- La clave consiste en una cadena de bits, con la cual se puede aplicar One Time Pad

QKD-BB84 (cont.)

La idea es transmitir una clave binaria por un canal inseguro.

QKD-BB84 (cont.)

La idea es transmitir una clave binaria por un canal inseguro.

Para transmitir el bit 0, Alice (el emisor) puede elegir al azar la base $\{|0\rangle, |1\rangle\}$ (a la que llamaremos esquema $+$) y considerar $0 \equiv |0\rangle$, o la base $\{|-\rangle, |+\rangle\}$ (a la que llamaremos esquema $\times$) y considerar $0 \equiv |-\rangle$. Analogamente al bit 1 lo codificamos como $|1\rangle$ en el esquema $+$ o como $|+\rangle$ en el esquema $\times$.

Bob realizará una medición sobre el estado recibido eligiendo al azar entre el esquema $+$ y el esquema $\times$.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

3: Alice le transmite a Bob la sucesión de esquemas empleadas.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

3: Alice le transmite a Bob la sucesión de esquemas empleadas.

4: Bob le informa a Alice en qué casos adivinó el esquema de origen.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

3: Alice le transmite a Bob la sucesión de esquemas empleadas.

4: Bob le informa a Alice en qué casos adivinó el esquema de origen.

5: Usando solamente los bits de los esquemas idénticos a dos puntas, ambos han definido una sucesión aleatoria de bits que servirá como one-time pad de encriptación para transmisiones futuras por cualquier canal.

QKD-BB84 (cont.)

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

3: Alice le transmite a Bob la sucesión de esquemas empleadas.

4: Bob le informa a Alice en qué casos adivinó el esquema de origen.

5: Usando solamente los bits de los esquemas idénticos a dos puntas, ambos han definido una sucesión aleatoria de bits que servirá como one-time pad de encriptación para transmisiones futuras por cualquier canal.

6: Alice y Bob intercambian hashes de las claves (en bloques) para aceptarla o descartarla.

QKD-BB84 (cont.)

Ejemplo:

Esquemas de Alice	$\times$	$+$	$+$	$\times$	$\times$	$+$
Valores de Alice	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$
Esquemas de Bob	$+$	$\times$	$+$	$\times$	$+$	$+$
Valores de Bob	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$
Coincidencias			$\surd$	$\surd$		$\surd$
Clave			0	1		0

QKD-BB84 (cont.)

Este protocolo es absolutamente inviolable.

QKD-BB84 (cont.)

Este protocolo es absolutamente inviolable.

Supongamos que Cliff espía el canal de comunicación entre Alice y Bob e intenta recuperar la clave. Cliff está en la misma situación que Bob y no conoce cuál esquema es el correcto, $+$ o $\times$. Por lo tanto elige al azar y se equivocará en promedio, la mitad de las veces.

QKD-BB84 (cont.)

Este protocolo es absolutamente inviolable.

Supongamos que Cliff espía el canal de comunicación entre Alice y Bob e intenta recuperar la clave. Cliff está en la misma situación que Bob y no conoce cuál esquema es el correcto, $+$ o $\times$. Por lo tanto elige al azar y se equivocará en promedio, la mitad de las veces.

En el paso 5 Alice y Bob se ponen de acuerdo en cuáles valores tomar en cuenta (las coincidencias de la secuencia de esquemas). Esta información no le sirve de nada a Cliff porque sólo en la mitad de las veces habrá usado el detector correcto, de manera que malinterpretará sus valores finales.

QKD-BB84 (cont.)

Además el QKD brinda el método para que Alice y Bob puedan detectar el potencial espionaje de Cliff:

Imaginemos que Alice envía un 0 con el esquema $\times$ ($|-\rangle$), Cliff usa el esquema $+$ forzando al qubit a definirse como $|0\rangle$ ó $|1\rangle$. Si Bob usa el esquema $\times$ y mide $|-\rangle$ coincide con lo enviado por Alice, pero si mide $|+\rangle$ Alice y Bob descubrirían esa discrepancia durante el intercambio de hashes, por lo tanto descartarían el bloque.

FIN

$$M_{\{|Preguntas?\rangle,|Gracias!\rangle\}} \frac{1}{\sqrt{2}}(|Preguntas?\rangle + |Gracias!\rangle)$$

FIN

$$M_{\{|Preguntas?\rangle,|Gracias!\rangle\}}\frac{1}{\sqrt{2}}(|Preguntas?\rangle + |Gracias!\rangle)$$

$$= |Gracias!\rangle$$