# Amarfly en el País de la Computación Cuántica

# Hola!

Women Techmakers

GDG Granada

## Soy *Ana Martínez Sabiote*

Estudiante de ingeniería Informática y Matemáticas en la Universidad de Granada

You can find me at anamarsabi@gmail.com

# Actualidad: supercomputadores

## Límites


Estos límites están impuestos por el modelo computacional que utilizamos. Es posible que, con un modelo computacional distinto, algunos de estos límites desaparezcan.

**Richard Feynmann**

*Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.*

# “Simulating” Physics

# QUBITS

BITS CUÁNTICOS

Concepto cuántico de bit de información.

Al igual que un bit, un qubit puede representar dos estados 0 y 1 (estados base)

ó

ambos estados de forma simultánea

## Conceptos básicos de mecánica cuántica

- Principio de Incertidumbre de Heisenberg
- Superposición de estados
- Entrelazado cuántico
- Coherencia

# Ejemplo: panda o cruz

# 100 ms

Tiempo de coherencia alcanzado actualmente

# QUBITS

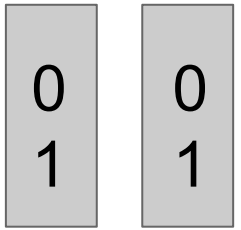
|0>

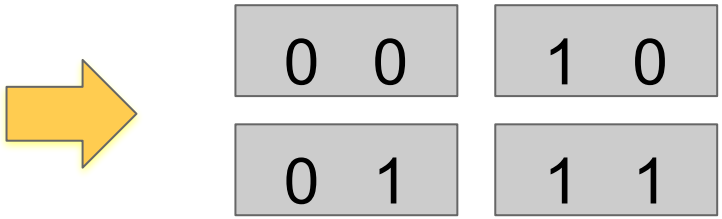
|1>

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

## PARALELISMO CUÁNTICO

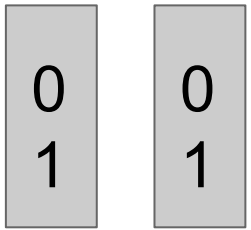
2 bits

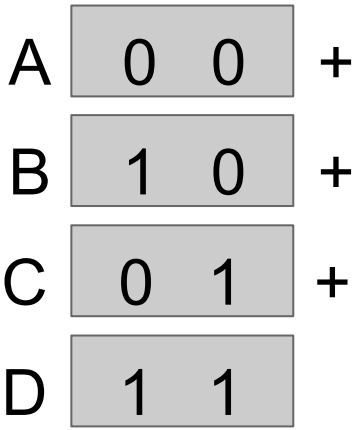



4 estados independientes. El sistema puede estar en uno de esos cuatro estados.

2 qubits



## Infraestructura física para qubits

Qubits de spin

Trampas de iones

Circuitos fototónicos

Computador cuántico topológico

Circuitos superconductores

# Características de este modelo de computación

## Puertas cuánticas

Equivalente a las puertas lógicas de los circuitos digitales.

Las puertas cuánticas son reversibles y matemáticamentes son matrices unitarias

# Puertas cuánticas, puertas unarias

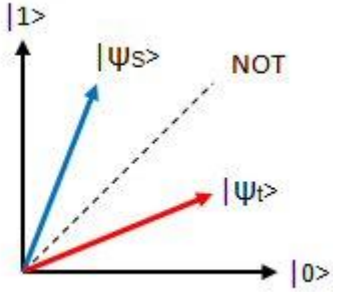
Puerta NOT

$$U_{NOT} = \sigma_1 = X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

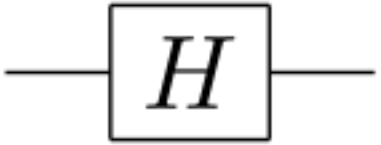
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\Psi_t\rangle = U_{NOT}|\Psi_s\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = b|0\rangle + a|1\rangle$$



# Puertas cuánticas, puertas unarias

## Puerta de Hadamard




$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(X + Z)$$

Transforma cualquiera de los estados base en una combinación de ambos. Rotación de π/2 radianes alrededor del eje X y del eje Z

El operador de Hadamard es una de las puertas cuánticas de mayor utilidad ya que realiza lo que se conoce como paralelismo masivo, ya que un estado de n qubits lo pone en superposición de $2^n$ estados.

## Puertas cuánticas, puertas unarias

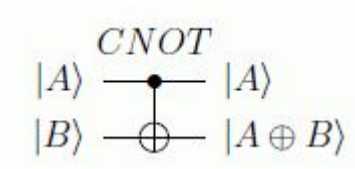
Puerta Z

$$Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Deja el estado fundamental inalterado ( |0> ) y cambia el signo del estado excitado ( |1> a -|1> )

# Puertas cuánticas múltiples

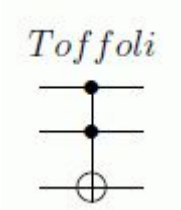
## Puerta CNOT




$$\left.\begin{aligned} |00\rangle &\longrightarrow |00\rangle \\ |01\rangle &\longrightarrow |01\rangle \\ |10\rangle &\longrightarrow |11\rangle \\ |11\rangle &\longrightarrow |10\rangle \end{aligned}\right\} \text{Puerta } CNOT$$

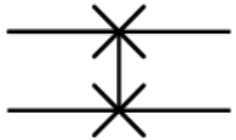
## Puerta de Toffoli

Extensión de tres qubits de la puerta CNOT.



# Puertas múltiples

Puerta SWAP



$$U_{\text{SWAP}} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

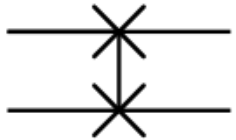
Intercambia los estados de dos qubits.

Puerta clonadora

$$U_{CLON}|b0\rangle = |bb\rangle \qquad \forall |b\rangle$$

# Puertas múltiples

Puerta SWAP



$$U_{\text{SWAP}} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Intercambia los estados de dos qubits.

Puerta clonadora

$$U_{CLON}|b0\rangle = |bb\rangle \qquad \forall |b\rangle$$

TEOREMA DE NO CLONACIÓN

## Qué resuelve la computación cuántica

- Problema del viajante
- Búsquedas no indexadas
- Factorización de grandes números

Transforma problemas con un crecimiento exponencial de la complejidad en problemas con un crecimiento polinómico.

# Algoritmos cuánticos

*Técnicas para la construcción de algoritmos cuánticos:*

- Amplificación de amplitud
- Transformada de Fourier cuántica
- Caminata cuántica
- Corrección cuántica de errores
- Simulación de sistemas físicos

Algoritmos cuánticos más significativos

Algoritmo de Deusch

Algoritmo de Grover

Algoritmo de Shor

# Algoritmo de Grover

Búsqueda en un espacio de datos no ordenado.

Modelo clásico

Tamaño espacio de datos=N

Evaluar búsqueda al menos N/2 intentos, N en el peor de los casos

Modelo cuántico

√N intentos

## Algoritmo de Shor

1123 x 919 = 1123937

1123937 = p x q → La base del algoritmo RSA radica en el problema de la factorización.

p y q son dos números primos del orden de $10^{200}$

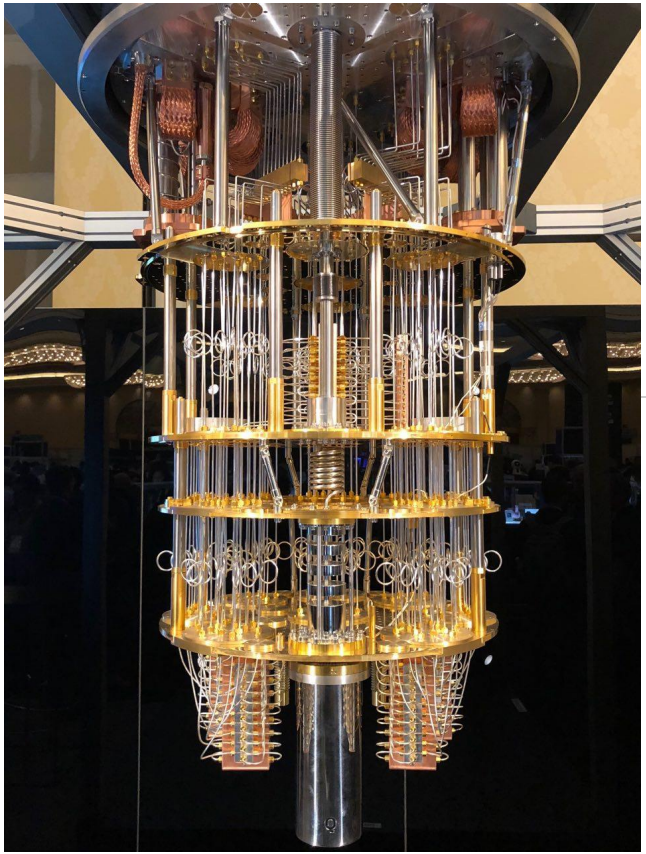
## Algoritmo de Shor

Descomponer un número N en sus factores primos por un computador clásico:

complejidad exponencial

En 2001 se ejecutó el algoritmo de Shor en un computador cuántico de 7 qubits.

# Computador cuántico



# 15 mK

El punto más frío del Universo

## Líneas de computación cuántica

Computación cuántica adiabática

DWave

Computador cuántico universal

# Supremacía cuántica

## Expectativas de la computación cuántica

Seguridad: encriptación postcuántica

Química, medicina y nuevos materiales

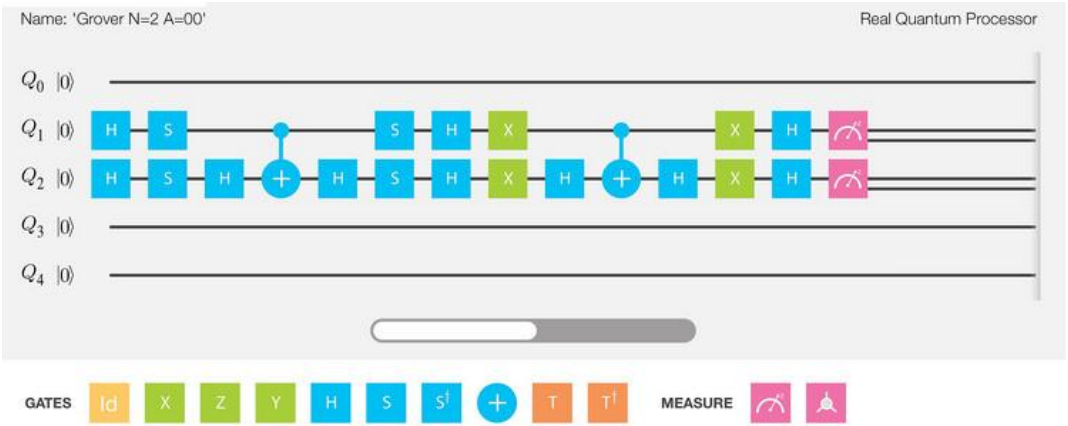
Machine learning y deep learning

Big data

Quantum internet

# Herramientas de programación

- Q#
- QuTiP : Quantum Toolbox in Python
- QISKit – IBM Quantum Experience



# Gracias!

## *Alguna pregunta ?*

You can find me at

- @IngenierasUGR
- anamarsabi@gmail.com