# QUANTUM COMPUTING

JORNADA DE DIVULGACIÓN DE APLICACIONES CIENTÍFICAS SOBRE PROCESADORES GRÁFICOS Y QUANTUM COMPUTING

## JGPUQC 2024 – UNIVERSIDAD DE ALICANTE

Manuel Benavent-Lledó <mbenavent@dtic.ua.es>

David Mulero-Pérez <dmulero@dtic.ua.es>

José García-Rodríguez <jgarcia@dtic.ua.es>

# Quantum Computing Reality

## Before we start...

Quantum Computing **HYPE**

- wild claims and promises
- talk of revolutions and paradigms shifts
- huge venture capital investment

  (9/10 are expected to fail)

Quantum Computing **REALITY**

- noisy/imperfect devices with ~100 qubits
- running particular tasks
- exascale classical HPC for verification
- <u>potential is real, even for early hardware</u>

08-04-2023

**Quantum computer built by Google can instantly execute a task that would normally take 47 years**

**Google, IBM make strides toward quantum computers that may revolutionize problem solving**

By Scott Pelley
December 3, 2023 / 7:17 PM EST / CBS News

NEW TECHNOLOGIES-INNOVATION

**Quantum computing the new milestone that will shake up the course of human history**

Quantum computing is one of the transformative technological trends that promises to change the world by quickly and efficiently solving impossible problems

# Why?

## Before we start...

Everyday computers – The ones we see

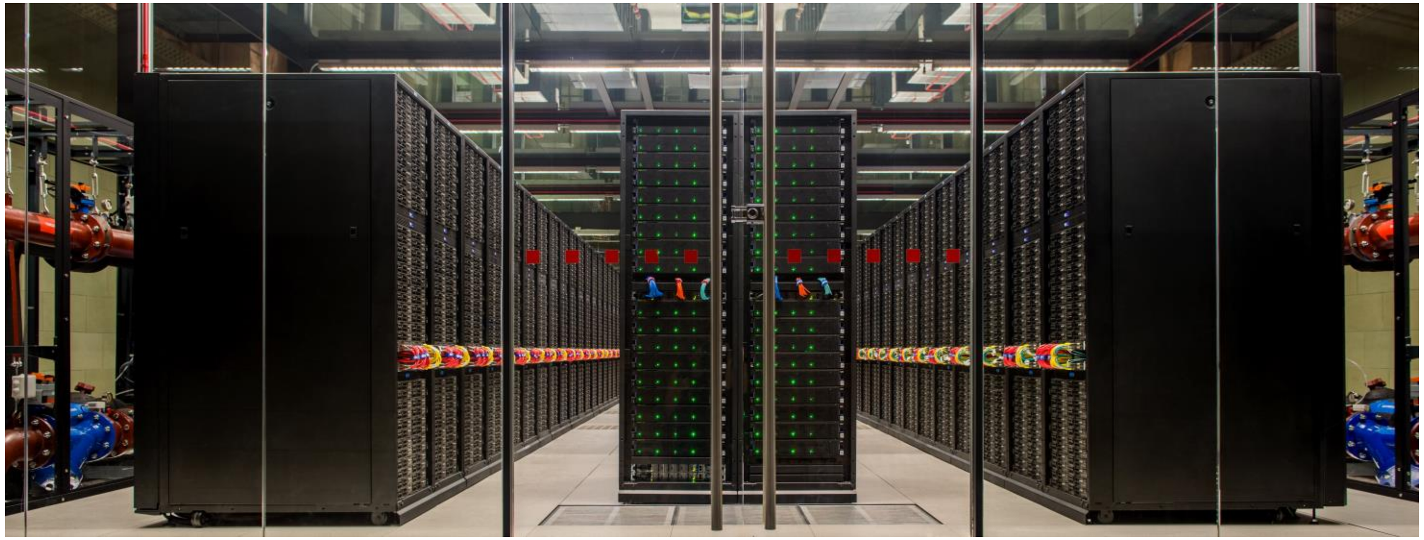
- Phones, Laptops
  - Batteries are helpful to reduce load BUT still need repair, recycle,...
- Desktop computers
  - Fancy graphics, Computer games,...
  - We can afford to “waste” power
    - Dual RTX 4090 requires 2kW
    - Gaming PC 1 kW on average
    - “Normal” computers 400-800W

# Why?

## Before we start…

Everyday computers – The ones we **DON'T** see

- Networks and data centers are on 24/7
- Provider services such as TV and Internet
    - In 2020, 4% of global electricity was used by networked devices
        - 6% including TV and other devices
- HPC uses MW of power (equivalent to a small town)

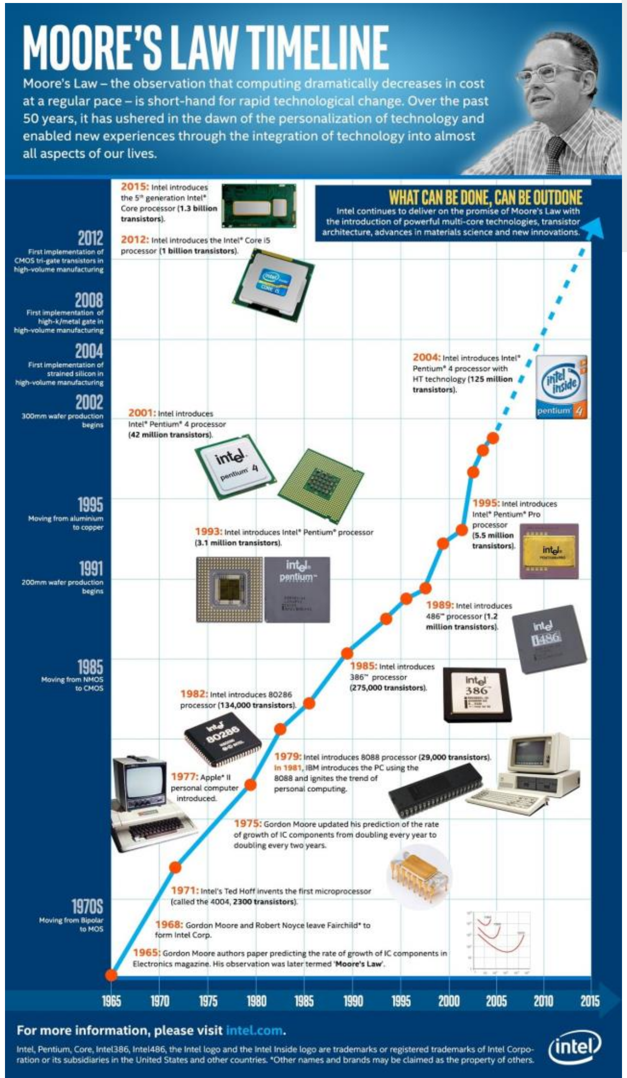


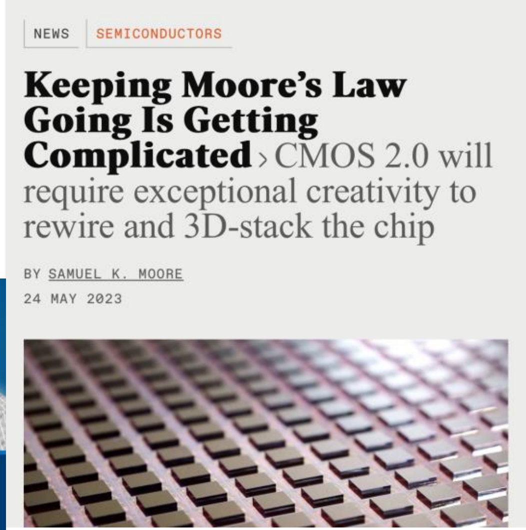
- MareNostrum4 (2017)
- 48 computing racks with a peak use of 33,7kW
- Network (6 switches 9,4kW)

https://www.bsc.es/es/marenostrum/marenostrum/informacion-tecnica

# Why?

## Before we start…





NEWS | SEMICONDUCTORS

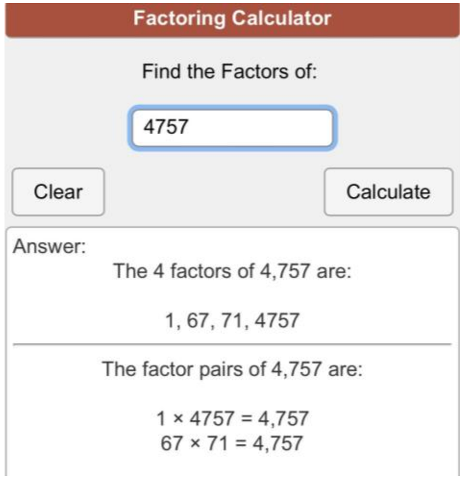
**Keeping Moore's Law Going Is Getting Complicated** › CMOS 2.0 will require exceptional creativity to rewire and 3D-stack the chip

BY SAMUEL K. MOORE

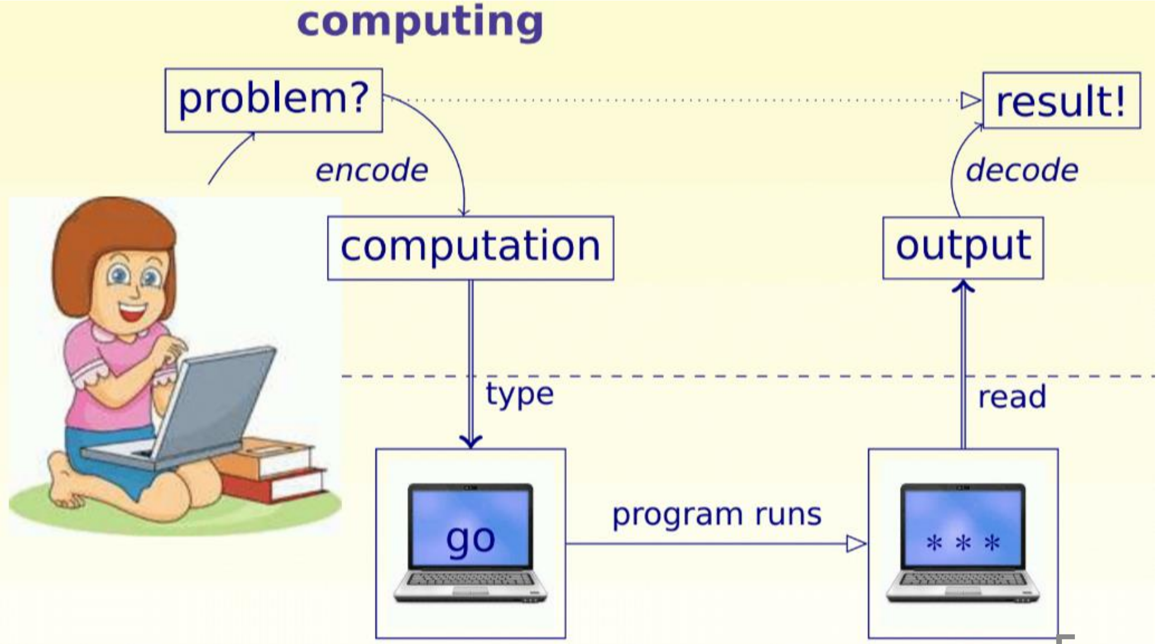
24 MAY 2023

**Besides…**

- Public Key Cryptography
- Banks and Governments interests




- Silicon chips can't be cooled any faster
- Quantum Computers?
- Hybrid computers?

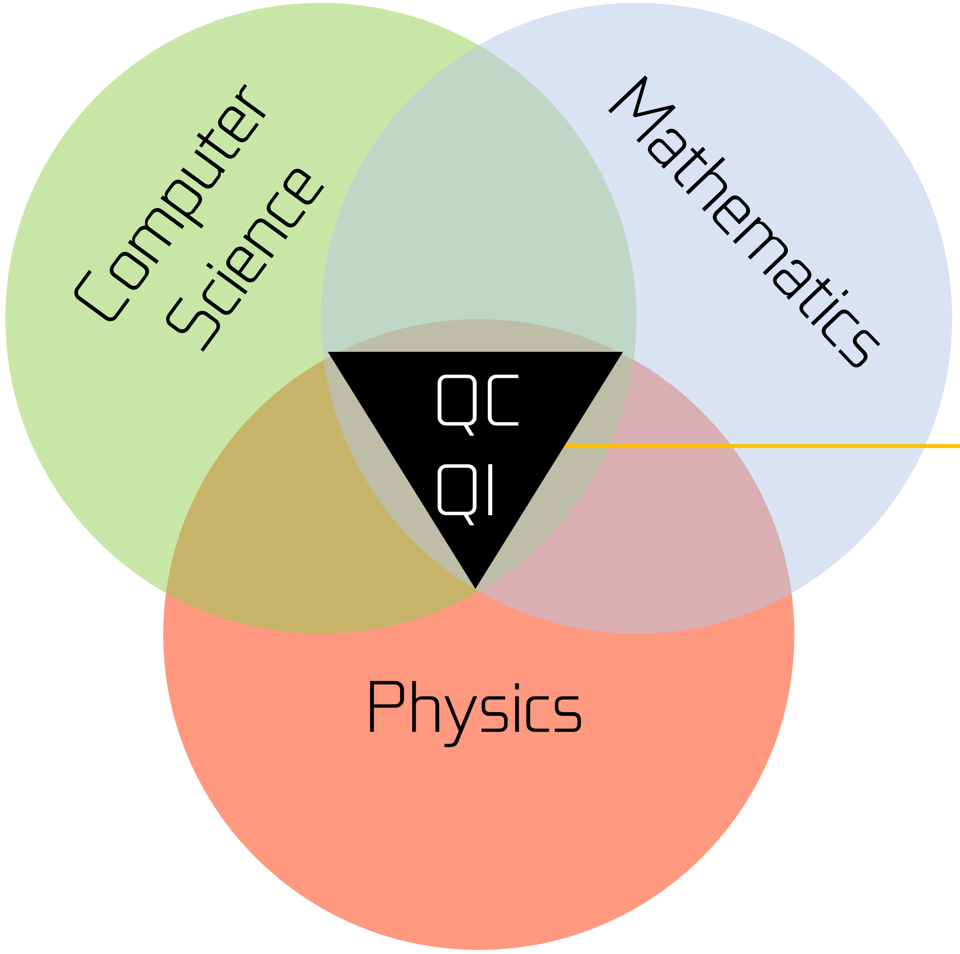


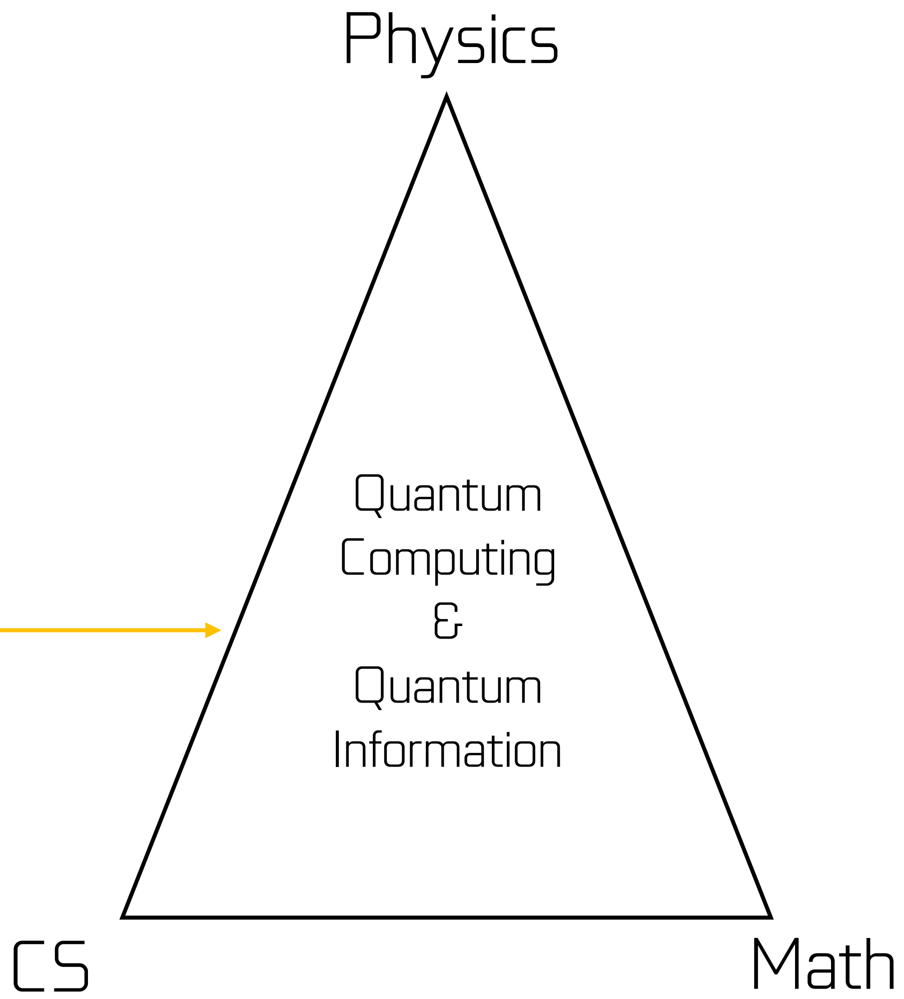

*When does a physical system compute?*
Horsman Dominic, Stepney Susan, Wagner Rob C. and Kendon Viv 2014
Proc. R. Soc. A.

# CONTENTS

# What is it?

## Quantum Computing



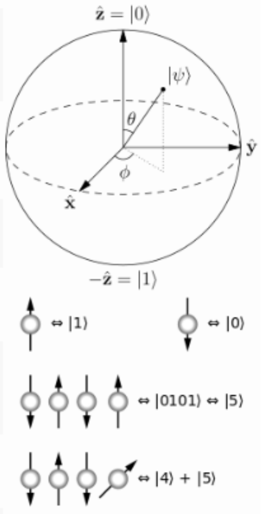
# What is it?

## Quantum Computing

V · T · E **Quantum information science** [hide]

| | | |
|---|---|---|
| **General** | | DiVincenzo's criteria · NISQ era · Quantum computing (Timeline) · Quantum information · Quantum programming · Quantum simulation · Qubit (physical vs. logical) · Quantum processors (Cloud-based) |
| **Theorems** | | Bell's · Eastin–Knill · Gleason's · Gottesman–Knill · Holevo's · Margolus–Levitin · No-broadcasting · No-cloning · No-communication · No-deleting · No-hiding · No-teleportation · PBR · Threshold · Solovay–Kitaev · Purification |
| **Quantum communication** | | Classical capacity (entanglement-assisted · Quantum capacity) · Entanglement distillation · Monogamy of entanglement · LOCC · Quantum channel (Quantum network) · Quantum teleportation (Quantum gate teleportation) · Superdense coding |
| | **Quantum cryptography** | Post-quantum cryptography · Quantum coin flipping · Quantum money · Quantum key distribution (BB84 · SARG04 · other protocols) · Quantum secret sharing |
| **Quantum algorithms** | | Amplitude amplification · Bernstein–Vazirani · Boson sampling · Deutsch–Jozsa · Grover's · HHL · Quantum annealing · Quantum counting · Quantum Fourier transform · Quantum optimization · Quantum phase estimation · Shor's · Simon's · VQE |
| **Quantum complexity theory** | | BQP · EQP · QIP · QMA · PostBQP |
| **Quantum processor benchmarks** | | Quantum supremacy · Quantum volume · Randomized benchmarking (XEB) · Relaxation times ($T_1$ · $T_2$) |
| **Quantum computing models** | | Adiabatic quantum computation · Continuous-variable quantum information · One-way quantum computer (cluster state) · Quantum circuit (Quantum logic gate) · Quantum machine learning (Quantum neural network) · Quantum Turing machine · Topological quantum computer |
| **Quantum error correction** | | Codes (CSS · Quantum convolutional · stabilizer · Shor · Steane · Toric · *gnu*) · Entanglement-assisted |
| **Physical implementations** | **Quantum optics** | Cavity QED · Circuit QED · Linear optical QC · KLM protocol |
| | **Ultracold atoms** | Optical lattice · Trapped ion QC |
| | **Spin-based** | Kane QC · Spin qubit QC · NV center · NMR QC |
| | **Superconducting quantum computing** | Charge qubit · Flux qubit · Phase qubit · Transmon |
| **Quantum programming** | | OpenQASM-Qiskit-IBM QX · Quil-Forest/Rigetti QCS · Cirq · Q# · libquantum · many others... |

Quantum information science · Quantum mechanics topics




qubits can be in a superposition of all the clasically allowed states

V · T · E **Quantum mechanics** [show]

V · T · E **Branches of physics** [show]

# Classic vs. Quantum

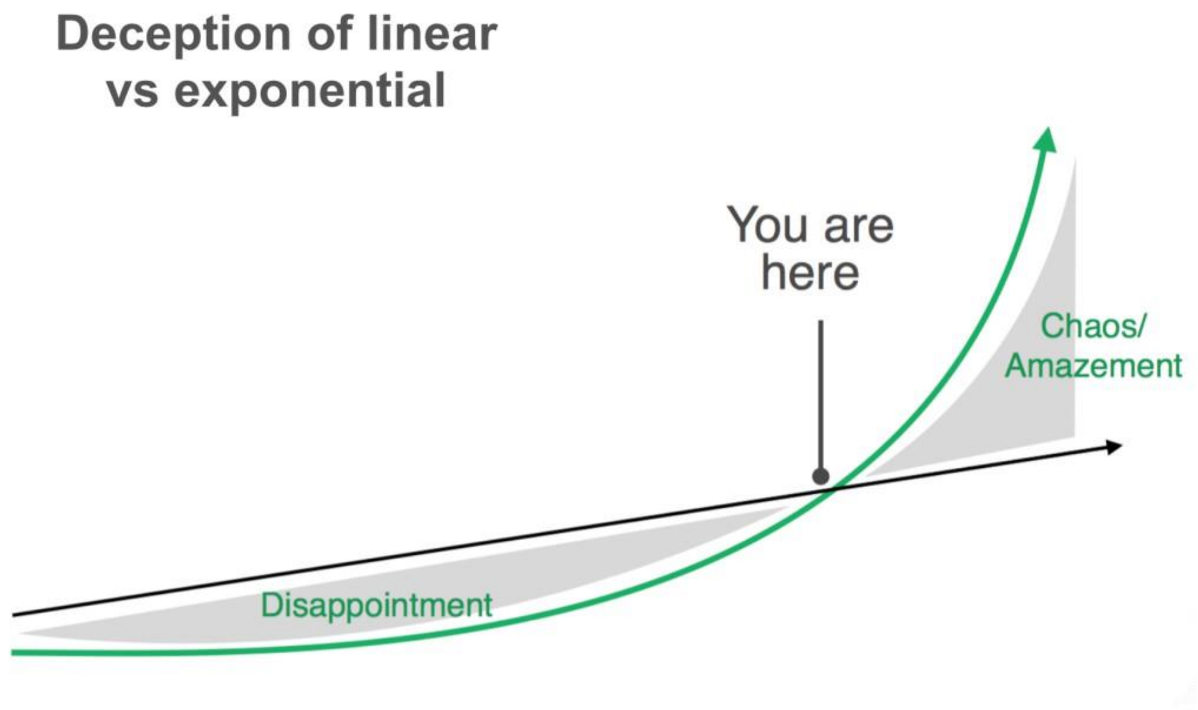
## Quantum Computing

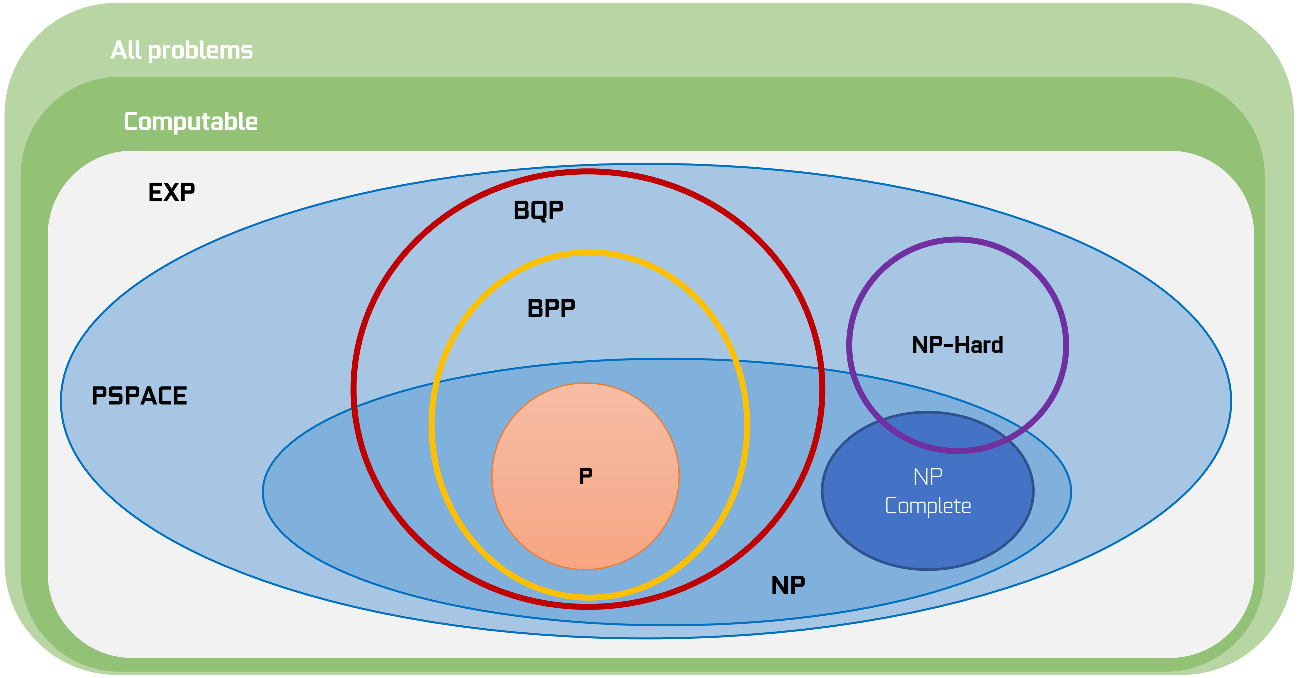
Complex physics experiment?

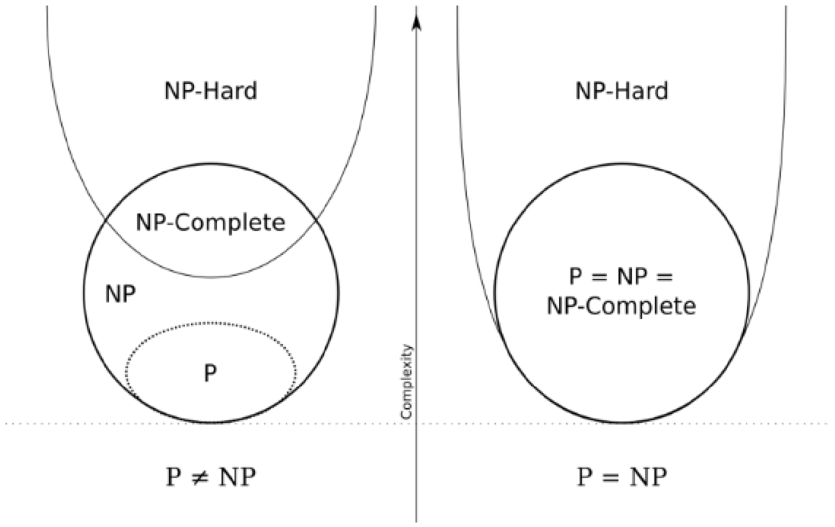
| | Classic | Quantum |
|---|---|---|
| Information | Binary | Binary |
| Registry | Single value | Multiple value |
| Operations | Sequential (except multicore or GPU) | Per value<br>Unlimited paralellism? |
| Error rates | Low | High |
| Operating Temperature | Room | Extremely low |
| Ideal use | Everyone, daily | Optimization, analysis and simulations |

# Quantum SpeedUp

## Quantum Computing



# Evolution

## Quantum Computing

Quantum Mechanics
1900-50

Benioff: Quantum Turing Machine
Feynman: Quantum Computer
1981-82

BB84 Protocol (QKD)
Deutch Algorithm
1984-85

"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."

**Richard P. Feynman**, *Simulating physics with computers* (1981)

Deutch-Josza Algorithm
Simon Algorithm
Quantum Teleportation
1992-93

1st experimentatial demonstration
1st controlled quantum state
1998-2000

1st quantum
encryption
2007

# Evolution

## Quantum Computing

John Preskill defines quantum supremacy (arxiv:1203.5813)

2012

Experimental demonstration with 50 qubits

2016

Google & Quantum Supremacy

2018-19

"This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy for this specific computational task, heralding a much-anticipated computing paradigm."

**Arute et al.** *Nature* (Octubre 2019)

"Public" quantum computers
Over 100 qubits

2020-21

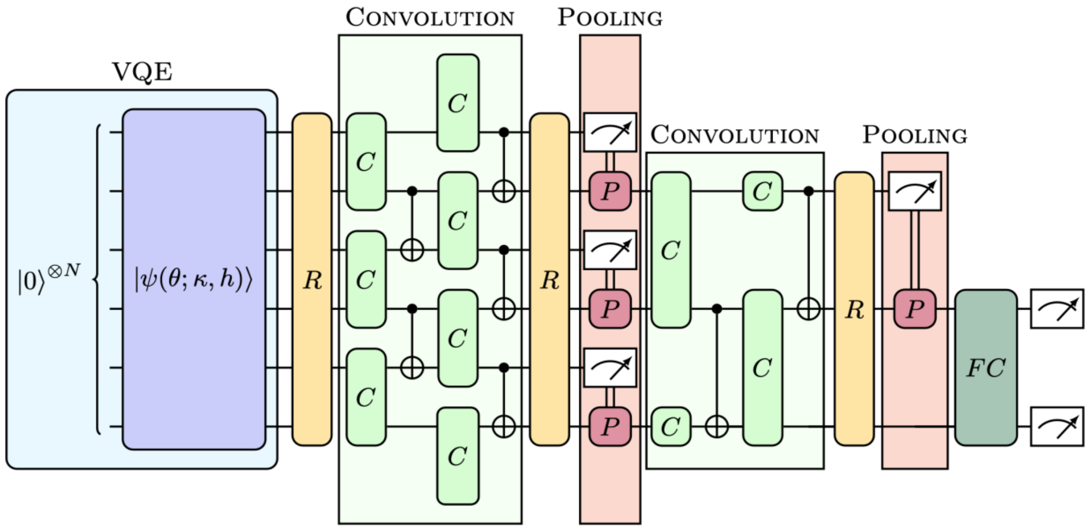
Technology under development
Reduced operations

Actualidad

# Applications

## Quantum Computing

- Cryptography
  - Simulation: modeling and simulating complex systems
  - Modeling complex systems
- Simulating physical systems (CERN -> HEP)
- Artificial Intelligence: Machine Learning and BigData
  - More efficiency and speed
- Optimization




Quantum Variational Encoder
arxiv:2208.08748

[Stock price prediction with Quantum Machine Learning compared to Keras (with code)]

# Bits and Qubits

## Mathematical Foundations

- Basic unit of information
- Bit (classic): 0 or 1
- Quantum:
  - Dirac Notation (Bra-Ket): $\langle\cdot| \; |\cdot\rangle$
  - Basis states: $|0\rangle$ o $|1\rangle$
  - State in superposition: $\alpha_0|0\rangle + \alpha_1|1\rangle$

$$|0\rangle = \binom{1}{0} \qquad |1\rangle = \binom{0}{1}$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0 \binom{1}{0} + \alpha_1 \binom{0}{1}$$

- Complex number in $\mathbb{C}^2$
- $\alpha_x \in \mathbb{C}$ (Amplitude)
- $|\alpha_x|^2$ = probability of collapsing to the state upon observation (measurement)

# Notation extension

## Mathematical Foundations

For $n$ qubits

- Vectors with base $\mathbb{C}^{2^n}$
- Dirac: $|0..0\rangle, |0..1\rangle, \ldots, |1..1\rangle$
- Tensor products of qubits
- $n = 2$

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

# Entanglement

## Mathematical Foundations

- **Product** state, can be represented as individual states

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

- Otherwise, **entangled** state:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

# Relevant states

## Mathematical Foundations

- Balanced superposition:

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

- **Bell state** (maximum entanglement):

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

# Classical VS. Quantum

## Mathematical Foundations

- **Bits**: Logic Gates
- NOT (Unitary)
- AND (Binary)
- OR (Binary)
- Etc.

**Qubits**: Quantum Gates

Properties:

- Basis state: define effect
- Superposition state: linearly
- Unitary
    - Previous properties
    - Reversible

# Quantum Gates

## Mathematical Foundations

Identity: most basic representation

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

$$|0\rangle = I \otimes |0\rangle = I|0\rangle = |0\rangle$$
$$|1\rangle = I \otimes |1\rangle = I|1\rangle = |1\rangle$$

**Pauli-X** = NOT

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

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

# Quantum Gates

## Mathematical Foundations

Other gates (not relevant for today)

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

**Hadamard**: creates a superposition

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

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

# Quantum Gates

## Mathematical Foundations

**CNOT**: Controlled NOT or CX

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow |a\ b\rangle = |a\ a \oplus b\rangle$$

$$CX|00\rangle = |00\rangle$$
$$CX|01\rangle = |01\rangle$$
$$CX|10\rangle = |11\rangle$$
$$CX|11\rangle = |10\rangle$$

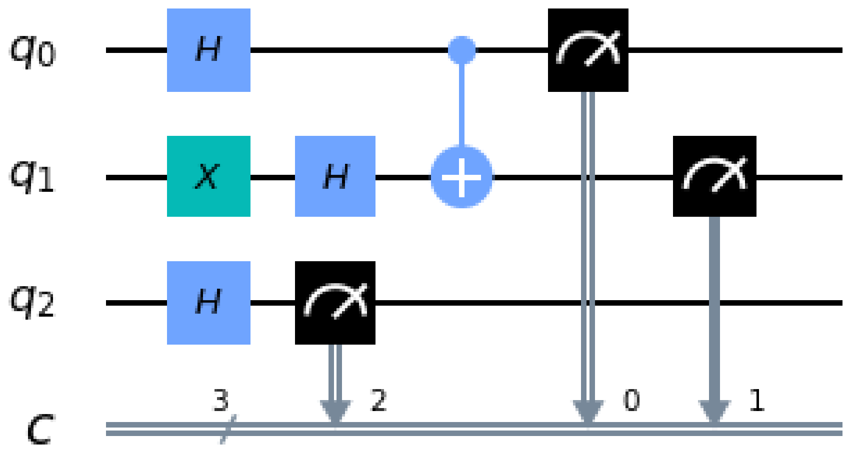
CCNOT: **Toffoli** gate

- Universality property as classical NAND gate

# Quantum Circuits

## Mathematical Foundations

- Link quantum gates
- **Representation**
  - Qubits: single cable
  - Bits: double cable
  - Gates: letters (sometimes symbols)

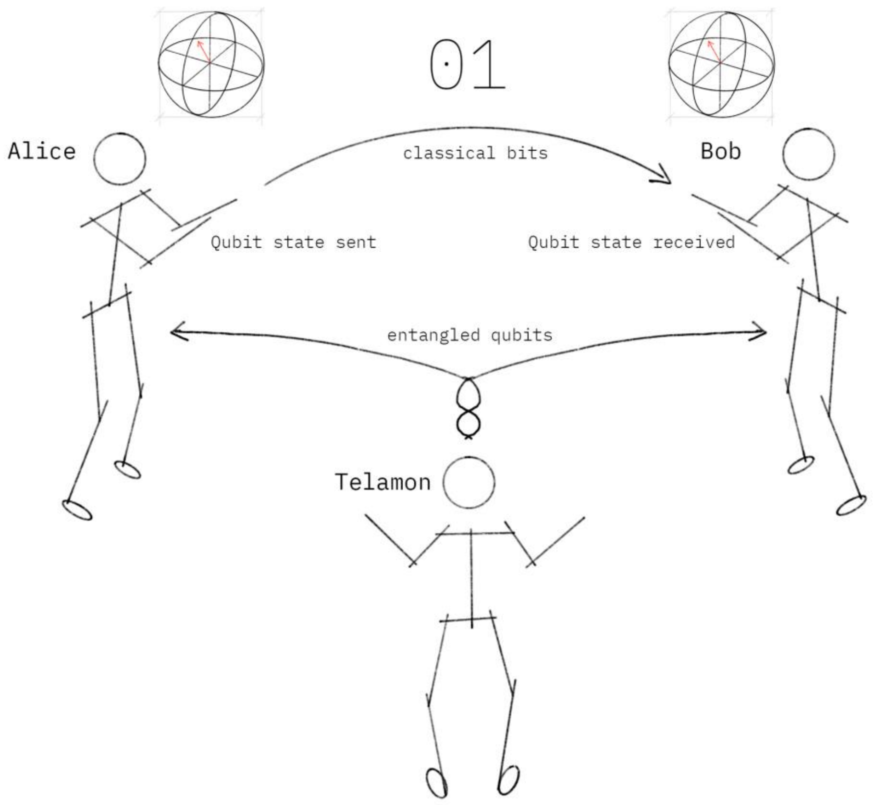



- Relevant gates in circuiits:
  - **Controlled-U**: controlled gate for operation (gate) U (generalization of CNOT)
  - **Measurement**: Observe qubit in a state $|\psi\rangle$, then it collapses into a bit according to its probability amplitudes

# Quantum Teleportation

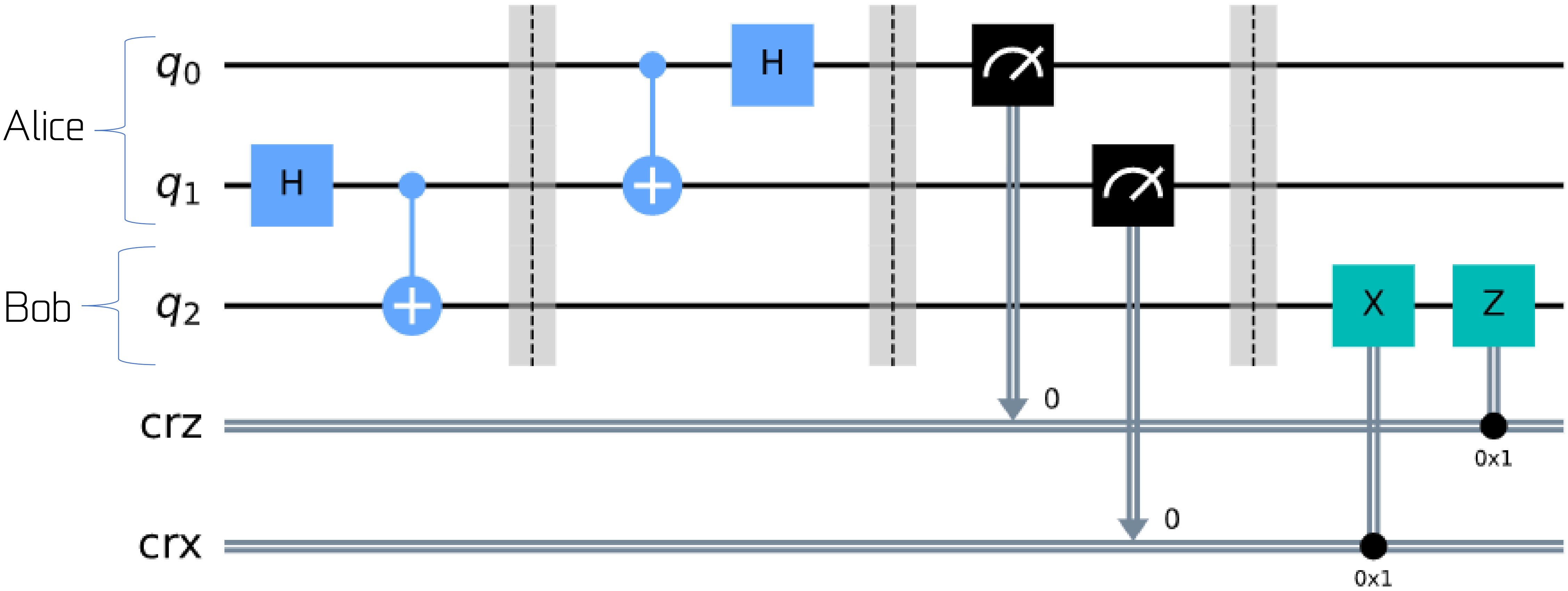
## Quantum Algorithms

- **Problem**: send 1 qubit using a classic channel
- Considerations:
  - Loss of information
  - Can't send complex number
  - No-cloning theorem
- **Solution:** Quantum teleportation
  - A 3rd person provides an entangled pair to A ar B
  - A operates its qubits
  - B "knows" how to get the original qubit thanks the bits send over the classical channel and the entangledqubit



# Quantum Teleportation

## Quantum Algorithms



# Deutsch-Jozsa Algorithm

## Quantum Algorithms

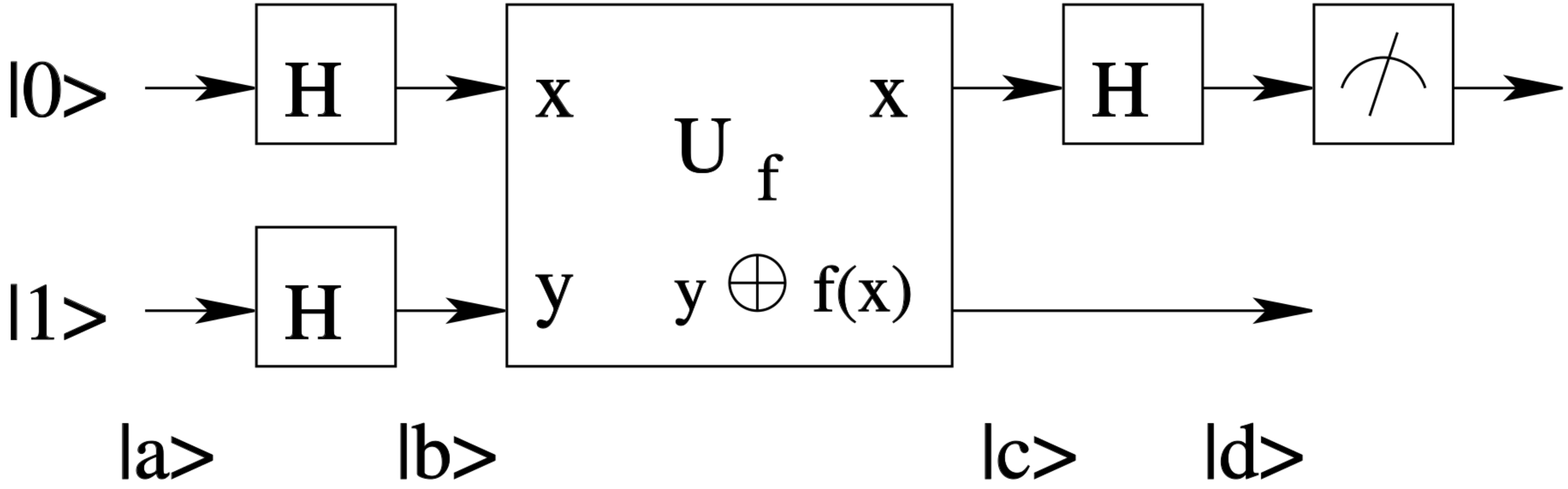
Deutsch Problem: an unknown function $f(x) = x \;\rightarrow \{0,1\}$ is:

- Balanced = same number of 0s and 1s.
- Constant = always 0 or always 1.

How do we determine the type of function with the minimum number of queries?

Classical computing needs N/2 + 1 queries

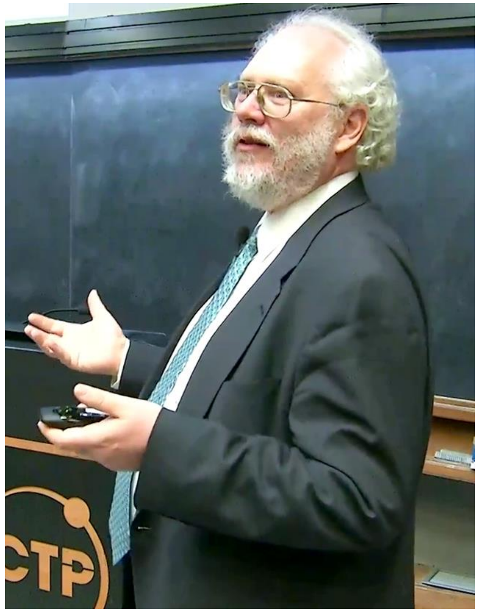
Quantum, one query will do:

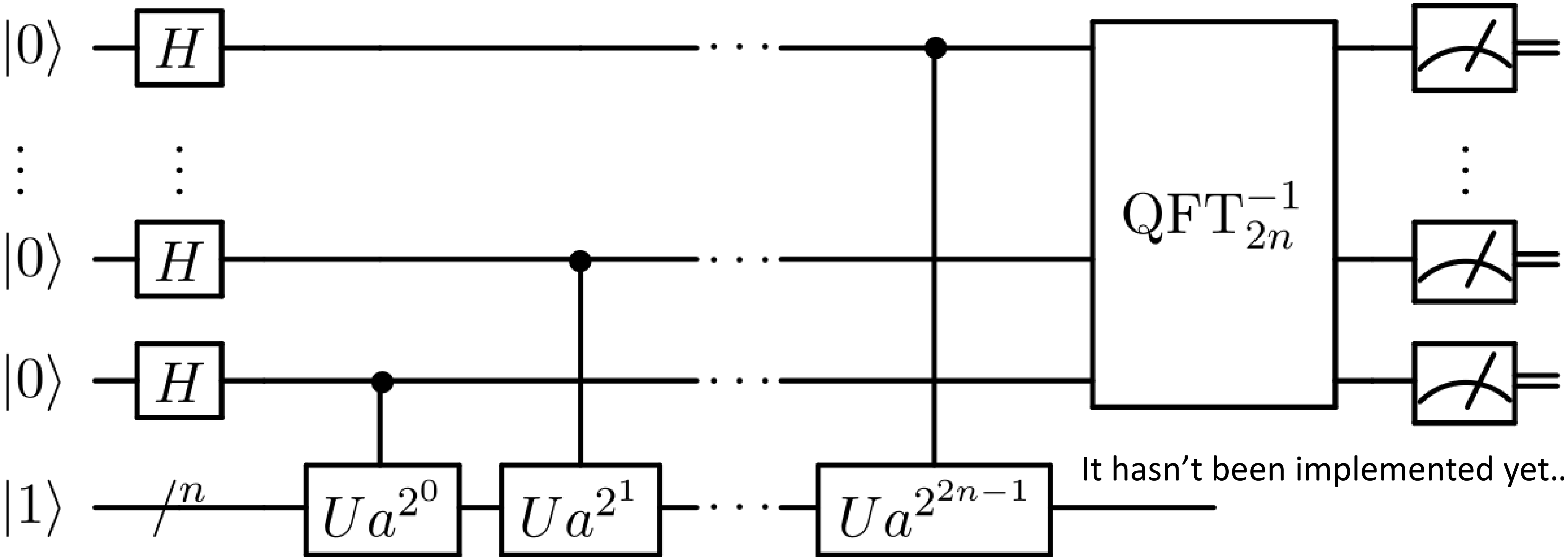


# Shor's Algorithm

## Quantum Algorithms

- Factoring numbers is hard, classically (RSA cryptography)
- The Fourier transforms are very useful but slow
- QFT offers an exponential improvement over FT




It hasn't been implemented yet…

# Summary of Relevant Algorithms

## Quantum Algorithms

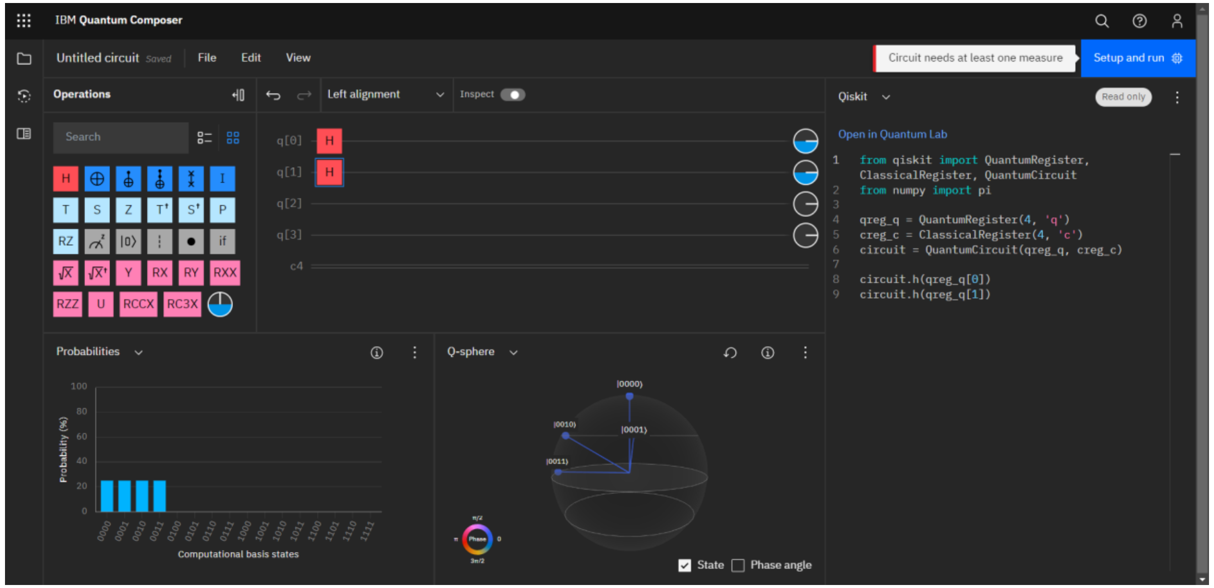
- **Deutsch-Josza**: first improvemnt over classical algorithms
    - **Bernstein-Vazirani**'s Algorithm
- **Simon**'s algorithm: exponential improvement over classical computers
    - Quantum Fourier Transform
- **Shor**'s algorithm: factoring numbers (RSA)
- **Grover**'s algorithm: unordered search with complexity $O(\log N)$
- **BB84** (Bennett-Brassard, 1984): basic quantum cybersecurity algorithm

# "QUANTUM PROGRAMMING"

## How do we program quantum computers?

Programming languages

- Python
  - Qiskit (IBM)
- Q# (Microsoft)
- Cirq (Google)




Differences with classic and conclusions:

- Under development
- Noisy systems
- Is it necessary a shift from the current paradigm?

# Any question?

## Some references:

- Curso Computación cuántica (YouTube), Eduardo Sáenz de Cabezón (Derivando): Parte 1 y Parte 2
- *Quantum Computation and Quantum Information*. Michael A. Nielsen & Isaac L. Chuang (Oxford 2010)
- *Quantum Computing Lecture Notes*. Ronald de Wolf, arXiv/1907.09415 (last update January 2023)
- *An Introduction to Quantum Computing*. Kaye, Phillip; Laflamme, Raymond and Mosca, Michele (Cambridge 2010)
- *Quantum Computing: A Gentle Introduction*. Rieffel, Eleanor and Polak, Wolfgang (MIT 2014)
- QuantumQ, Game available in Playstore

# QUANTUM COMPUTING

JORNADA DE DIVULGACIÓN DE APLICACIONES CIENTÍFICAS SOBRE PROCESADORES GRÁFICOS Y QUANTUM COMPUTING

## JGPUQC 2024 – UNIVERSIDAD DE ALICANTE

Manuel Benavent-Lledó <mbenavent@dtic.ua.es>

David Mulero-Pérez <dmulero@dtic.ua.es>

José García-Rodríguez <jgarcia@dtic.ua.es>

3dperceptionlab/jgpuqc2024

Qiskit Tutorial