QUANTUM COMPUTING

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

JGPUQC 2023 - UNIVERSIDAD DE ALICANTE

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

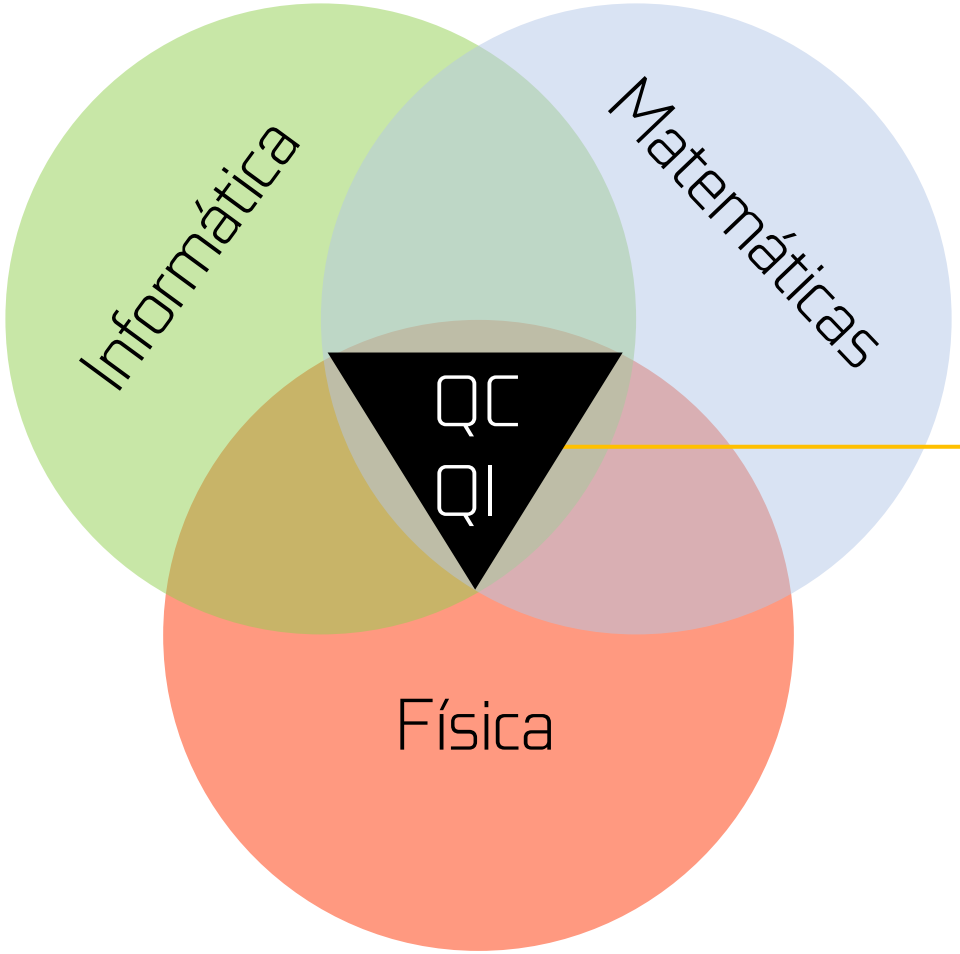
David Mulero-Pérez <dmulero@dtic.ua.es>

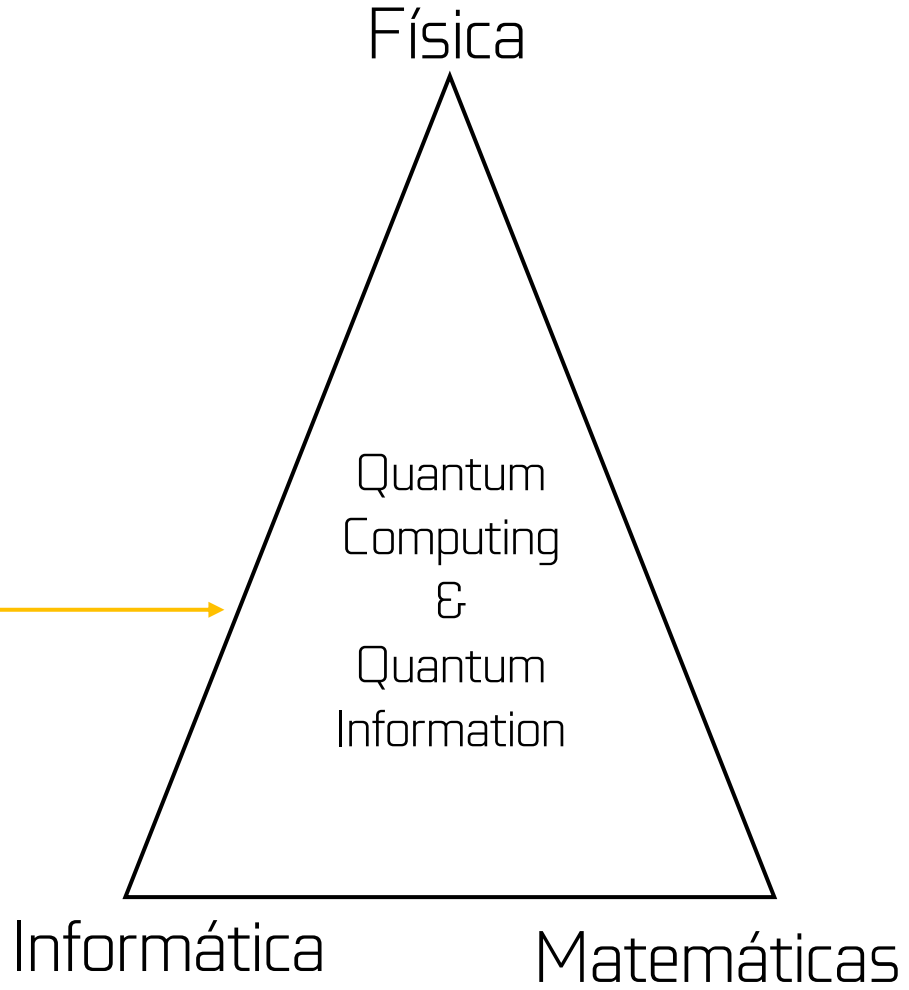
José García-Rodríguez <jgarcia@dtic.ua.es>

CONTENIDO

COMPUTACIÓN CUÁNTICA

¿En qué consiste?

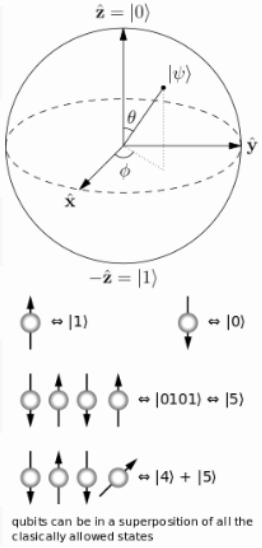




COMPUTACIÓN CUÁNTICA

¿En qué consiste?

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		



v · t · e	**Quantum mechanics**	[show]

v · t · e	**Branches of physics**	[show]

COMPUTACIÓN CUÁNTICA

Clásico vs Cuántico

ORDENADOR CLÁSICO

- Información binaria
- Registros con un único valor
- Ejecución secuencial con posibilidad de paralelizar (GPUs o varios núcleos)

¿Ordenador o experimento físico muy complejo?

ORDENADOR CUÁNTICO

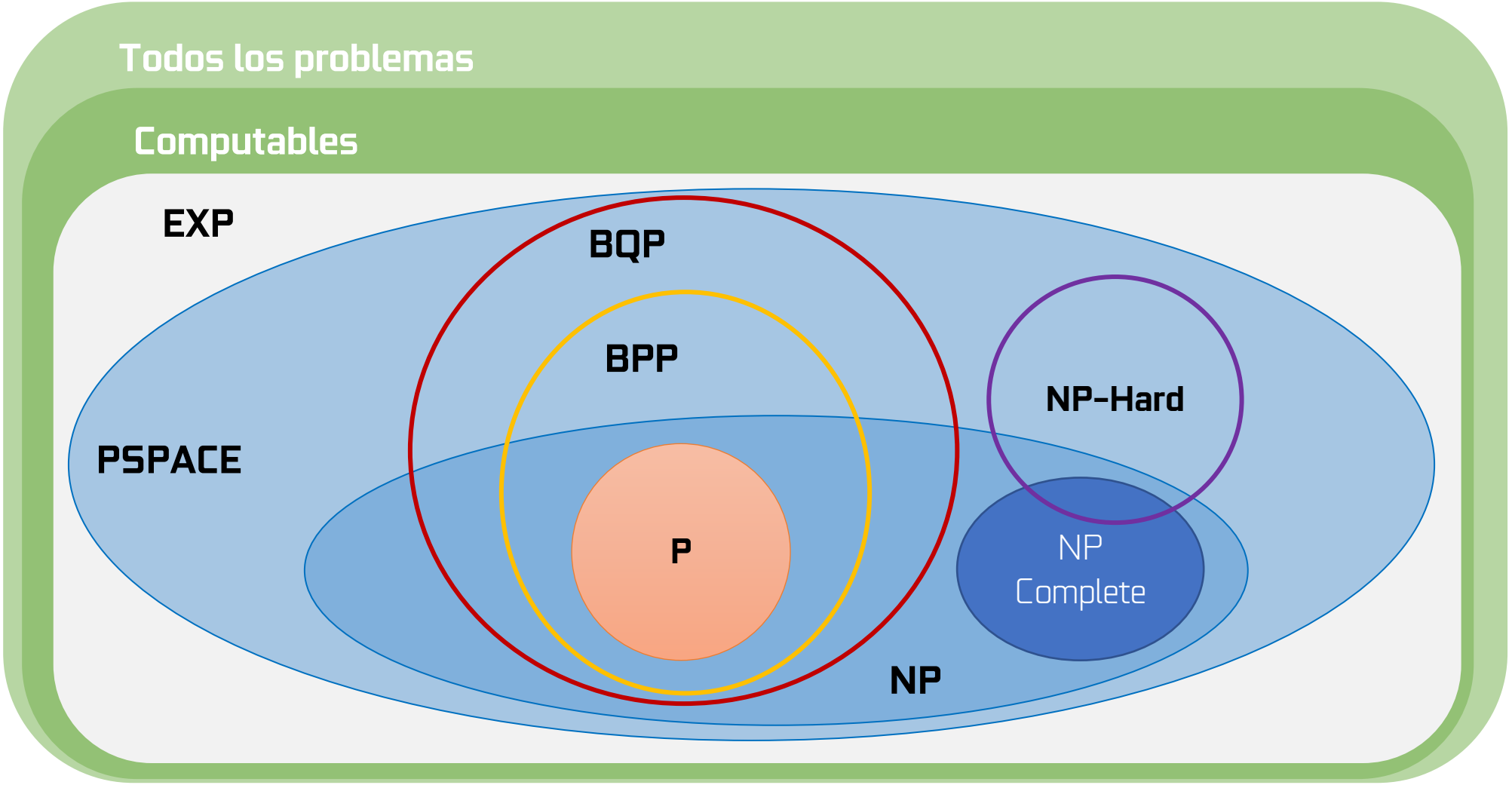
- Información binaria
- Registros con posibilidad de tener varios valores
- Operaciones en cada valor de cada registro

↓

Paralelismo ilimitado

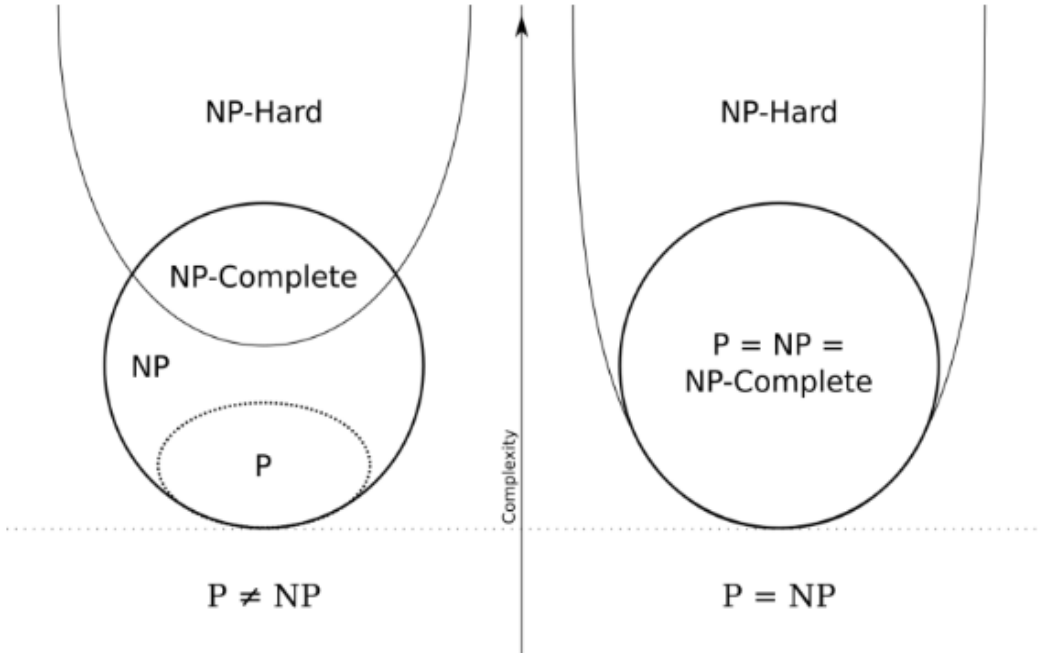
COMPUTACIÓN CUÁNTICA

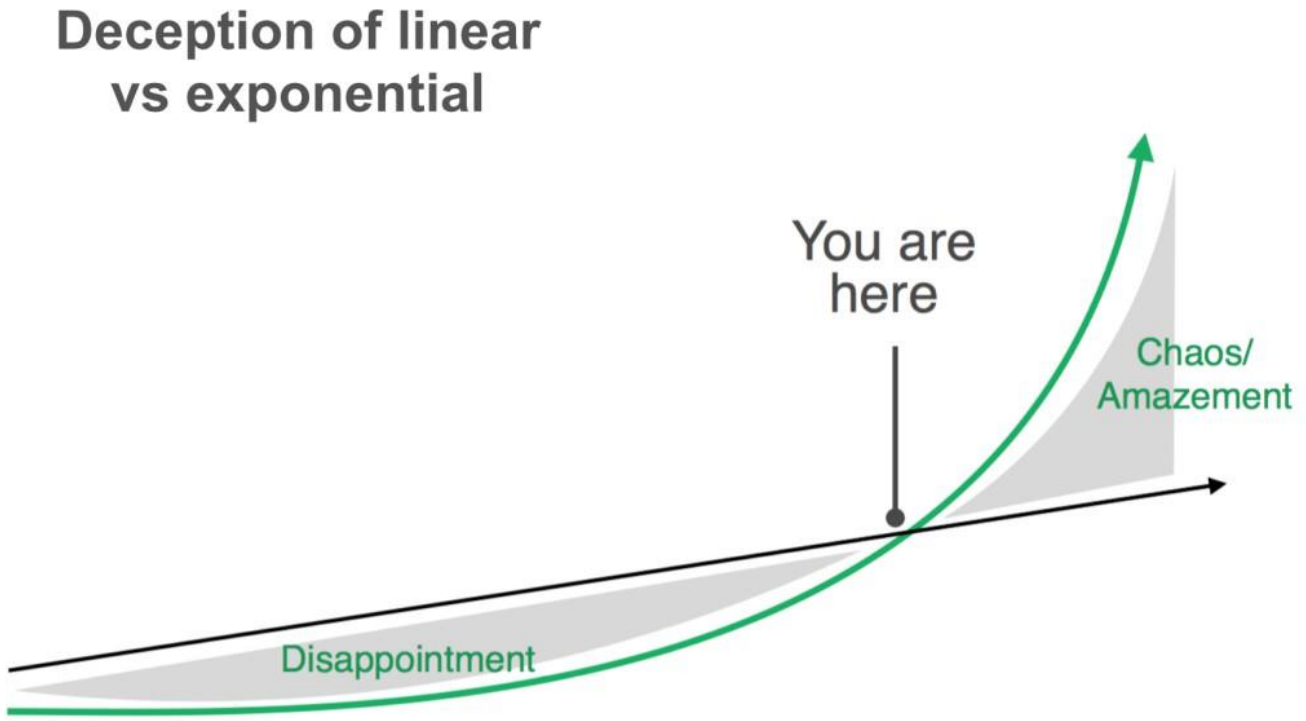
¿Aceleración Cuántica?



COMPUTACIÓN CUÁNTICA

¿Aceleración Cuántica?





COMPUTACIÓN CUÁNTICA

Evolución

Bases Mecánica Cuántica — 1900-50

→

Benioff: Quantum Turing Machine
Feynman: Ordenador cuántico — 1981-82

→

Protocolo BB84 (QKD)
Algoritmo de Deutch — 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)

Algoritmo de Deutch-Josza
Algoritmo de Simon
Teleportación Cuántica — 1992-93

→

1ª demonstración experimental
1º estado cuántico controlado — 1998-2000

→

1º Cifrado cuántico — 2007

COMPUTACIÓN CUÁNTICA

Evolución

John Preskill define la supremacía cuántica (arxiv:1203.5813)

2012

Demonstración experimental con 50 qubits

2016

Google y la supremacía cuántica

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)

Ordenadores cuánticos "comerciales"
Más de 100 qubits

2020-21

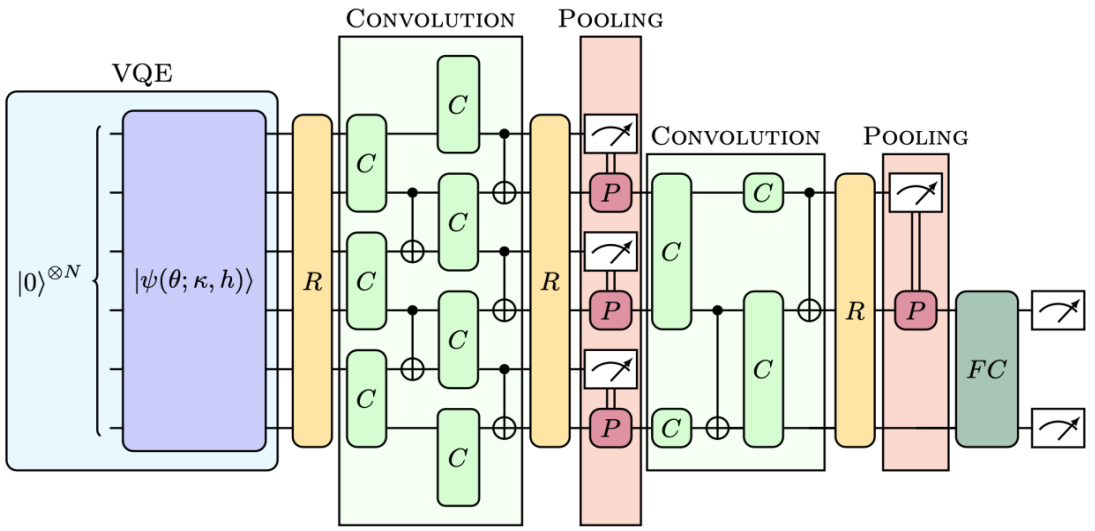
Tecnología en desarrollo
Operaciones reducidas

Actualidad

COMPUTACIÓN CUÁNTICA

Aplicaciones

1. Criptografía
2. Simulación: modelar y simular sistemas complejos
   - Modelar sistemas complejos
   - Simular sistemas físicos (CERN -> HEP)
3. Inteligencia Artificial: Aprendizaje Automático y BigData
   - Más eficiencia y velocidad
4. Optimización



Quantum Variational Encoder
arxiv:2208.08748

BASES MATEMÁTICAS: Introducción a la Mecánica Cuántica

Bits y Qubits

- Unidad básica de información
- Clásica: 0 o 1
- Cuántica:
  - Notación Dirac Bra-Ket: $\langle \cdot | \ | \ \cdot \rangle$
  - Estados básicos: $|0\rangle$ o $|1\rangle$
  - Estado en superposición: $\alpha_0|0\rangle + \alpha_1|1\rangle$

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

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Forman una base de $\mathbb{C}^2$: tienen parte compleja
- $\alpha_x \in \mathbb{C}$ (Amplitud)
- $|\alpha_x|^2 =$ probabilidad de colapsar al x al observar

BASES MATEMÁTICAS: Introducción a la Mecánica Cuántica

Extensión de la notación

Notación para n qubits

- Vectores de base $\mathbb{C}^{2^n}$
- Notación Dirac: $|0..0\rangle, |0..1\rangle, \ldots, |1..1\rangle$
- Bit más significativo a la izquierda
- Productos tensoriales de qubits
- Ejemplo para $n = 2$

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

En superposición: $\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$

Como producto tensorial: $|00\rangle = |0\rangle \otimes |0\rangle$

BASES MATEMÁTICAS: Introducción a la Mecánica Cuántica

Entrelazamiento

- Estado **producto**: estado que se puede poner como producto de sus componentes

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

- Sino, estado en **entrelazamiento**:

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

BASES MATEMÁTICAS: Introducción a la Mecánica Cuántica

Entrelazamiento: Estados importantes

- Superposición equiprobable:

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

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

- **Estado de Bell** (Par EPR: Einstein-Podolsky-Rosen)

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

BASES MATEMÁTICAS: Puertas Cuánticas

Clásica vs Cuántica

Bits: Puertas lógicas

- NOT (Unitaria)
- AND (Binaria)
- NAND (Binaria)
    - Propiedad universalidad (NOR)

Qubits: Puertas cuánticas

- Estado básico: definir su efecto
- Estado en superposición: actuación lineal
- Unitarias
    - Propiedades anteriores
    - Reversibles

BASES MATEMÁTICAS: Puertas Cuánticas

Puertas importantes

- Identidad, utilizada normalmente para demonstrar teoremas:

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

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

- **Pauli-X**: NOT clásico

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

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

BASES MATEMÁTICAS: Puertas Cuánticas

Puertas importantes

- Hay otras puertas relevantes: Z, Y, S (a veces P), ...

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

- **Hadamard**: pone a los qubits en estado de superposición

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

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

BASES MATEMÁTICAS: Puertas Cuánticas

Puertas importantes

- **CNOT**: Controlled NOT o CX

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

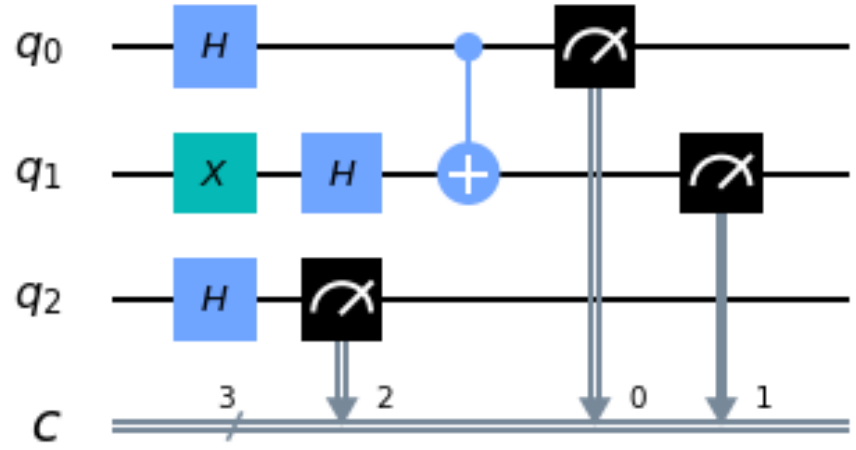
$$CX|00\rangle = |00\rangle$$
$$CX|01\rangle = |01\rangle$$
$$CX|10\rangle = |11\rangle$$
$$CX|11\rangle = |10\rangle$$

- CCNOT: **Toffoli** gate
  - Universalidad de puertas clásicas

BASES MATEMÁTICAS: Circuitos cuánticos

Básicos

- Concatenaciones de puertas cuánticas
- **Representación**
  - Qubits: un solo cable
  - Bits: doble cable
  - Puertas: letras o signo más para CNOT



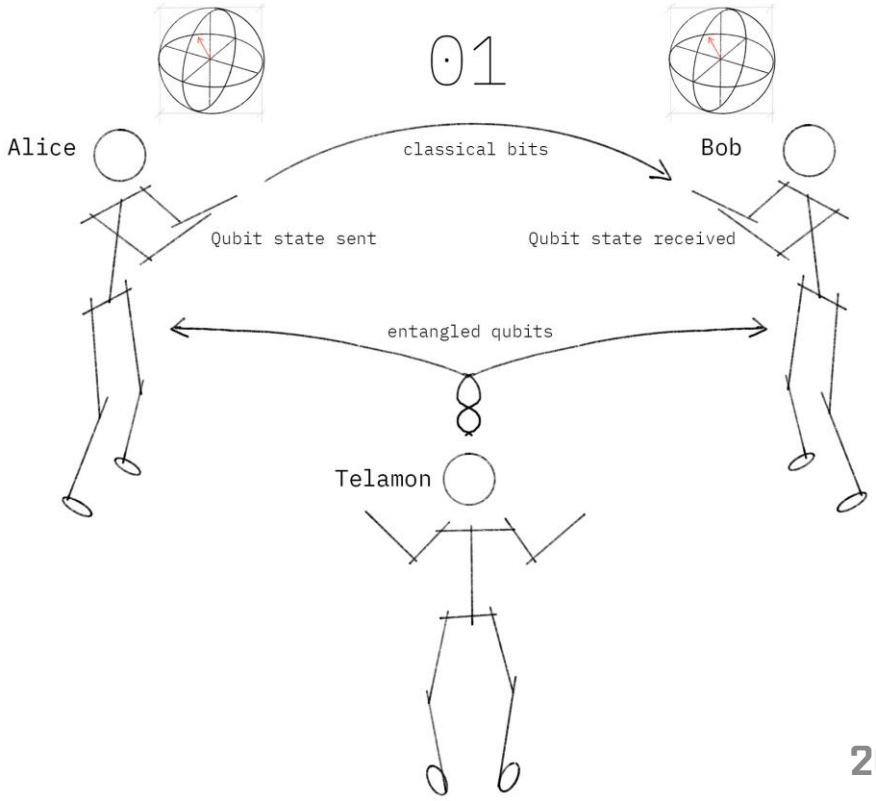
- Puertas cuánticas relevantes en circuitos:
  - **Controlled-U**: puerta de $n + 1$ qubits en la que se aplica un control a la operación U (CNOT aplicado al resto de casos)
  - **Medida**: Convierte un qubit en un estado $|\psi\rangle$ a un bit clásico según la probabilidad de sus amplitudes

BASES MATEMÁTICAS: Circuitos cuánticos

Avanzados: Teleportación cuántica

- **Problema**: enviar 1 qubit entre dos entidades, Alice y Bob, a través de un canal clásico
- Consideraciones:
  - Pérdida de información al medir
  - Envío de números complejos en canales clásicos
  - Teorema de la no clonación
- **Solución:** Quantum teleportation
  - Telamon da a Alice y Bob un estado entrelazado
  - Alice opera sobre sus qubits
  - Bob, al recibir los bits, sabe como operar su qubit

para obtener el estado de Alice



BASES MATEMÁTICAS: Circuitos cuánticos

Avanzados: Teleportación cuántica

- Inicialmente Alice tiene: $\alpha_0|0\rangle + \alpha_1|1\rangle$ y quiere enviarlo a Bob

- Telamon (3ª persona) da un qubit a Alice y Bob en estado EPR, es decir:

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Luego, Alice aplica CNOT y Hadamard a sus qubits quedando:

$\frac{1}{2}|00\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle) +$ Alice

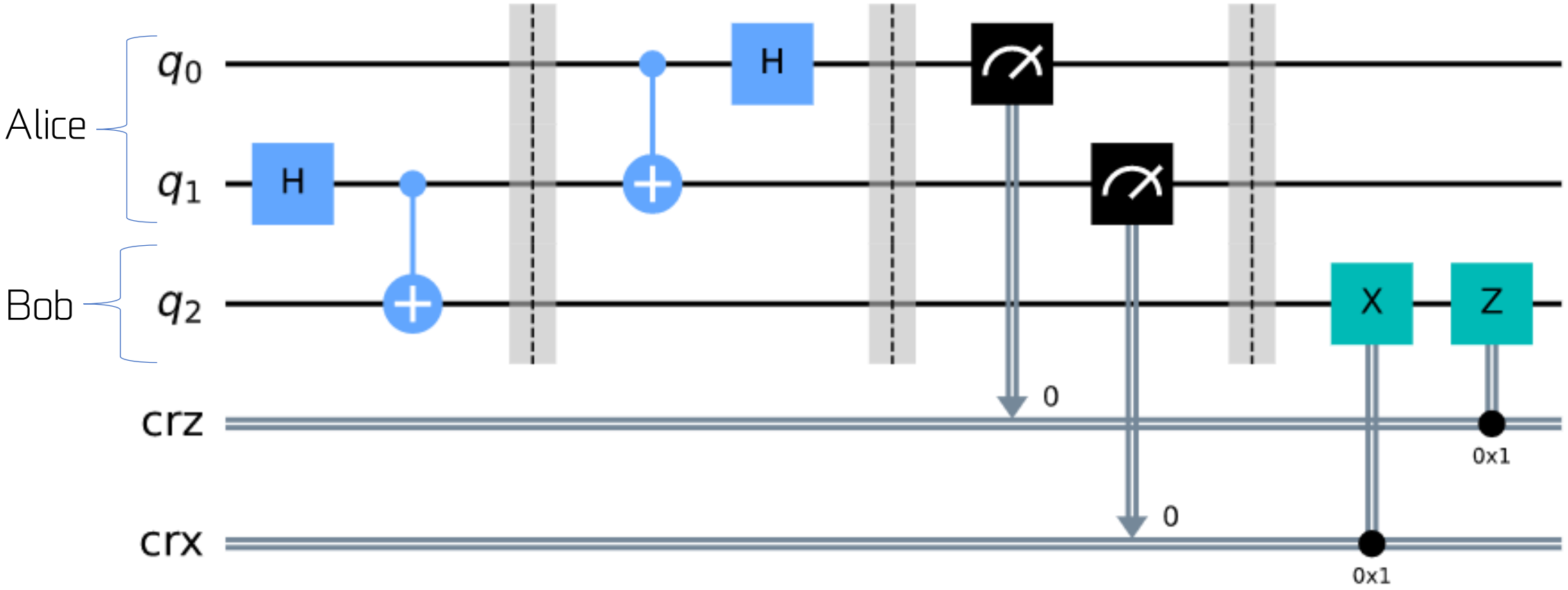
$\frac{1}{2}|01\rangle(\alpha_0|1\rangle + \alpha_1|0\rangle) +$ Alice negado (X)

$\frac{1}{2}|10\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle) +$ Alice con cambio de signo (Z)

$\frac{1}{2}|11\rangle(\alpha_0|1\rangle - \alpha_1|0\rangle)$ Alice negado (X) y con cambio de signo (Z)

BASES MATEMÁTICAS: Circuitos cuánticos

Avanzados: Teleportación cuántica



*Ejemplo en un mismo circuito, se puede hacer envío a través de cualquier canal clásico

BASES MATEMÁTICAS: Circuitos cuánticos

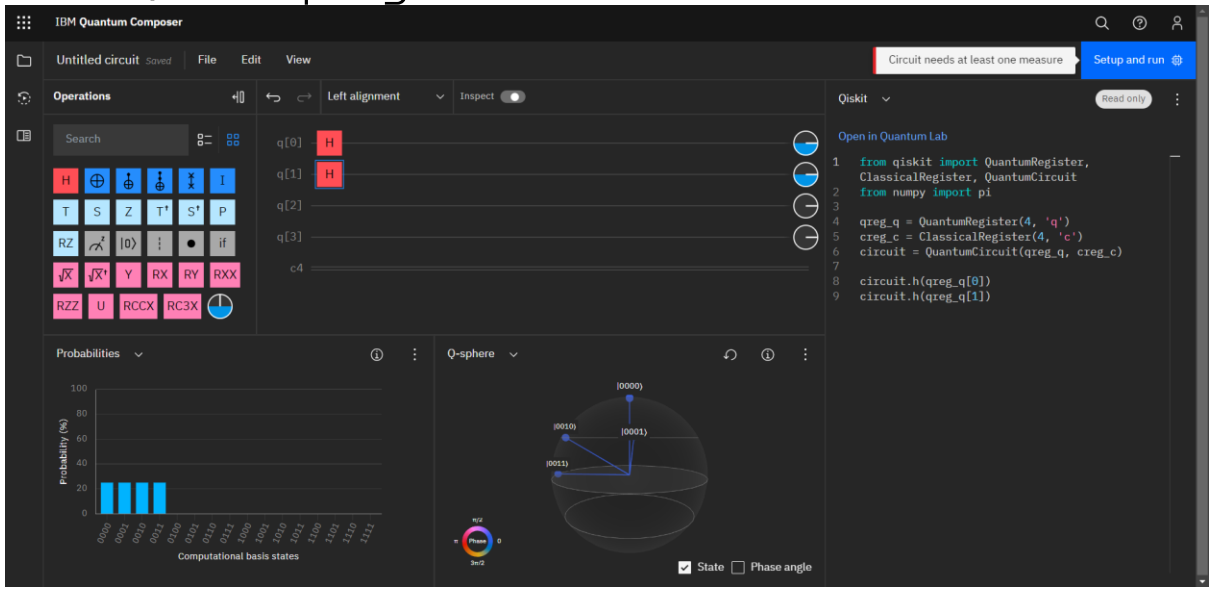
Avanzados: Algoritmos cuánticos

- Algoritmo de **Deutsch–Josza**: mejora sobre algoritmos clásicos
    - Algoritmo de **Bernstein–Vazirani**
- Algoritmo de **Simon**: mejora exponencial sobre algoritmos clásicos
    - Transformada de Fourier Cuántica
- Algoritmo de **Shor**: factorización de números primos (RSA)
- Algoritmo de **Grover**: búsqueda no ordenada en $O(\log N)$
- **BB84** (Bennett-Brassard, 1984): protocolo básico de seguridad cuántica

“PROGRAMACIÓN CUÁNTICA”

¿Podemos programar como lo conocemos?

- Lenguajes de programación
  - Python
    - Qiskit (IBM)
  - Q# (Microsoft)
  - Cirq (Google)
- ¿Qué se programa realmente?



Diferencias con la programación clásica:

- Tecnología en desarrollo
- Mucho ruido en los sistemas
- ¿Son los modelos actuales los definitivos o es necesario un cambio de paradigma?

¿PREGUNTAS?

Algunas referencias:

- 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 (última actualización enero 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, Juego disponible en PlayStore para resolver circuitos cuánticos

QUANTUM COMPUTING

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

JGPUQC 2023 - UNIVERSIDAD DE ALICANTE

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

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

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