cnrs SCIENCES INFORMATIQUES

Les algorithmes à l'ère du calcul quantique

Yassine Hamoudi

LaBRI
université de BORDEAUX
Hyb Quant
Maison du Quantique de Nouvelle-Aquitaine

A prototype quantum computer

IBM Quantum System Two (San Sebastian - Spain)

One of the foundational results in quantum computing:

Shor's algorithm (1994)

$65535 = 3 \times 5 \times 17 \times 257$

An extremely fast method for finding the prime factors of any number

… but which requires a quantum computer to run

Before Shor's algorithm:

Widely believed that no efficient algorithm would ever exist for this problem

… and much of cryptography relied on this assumption (e.g., RSA cryptosystem)

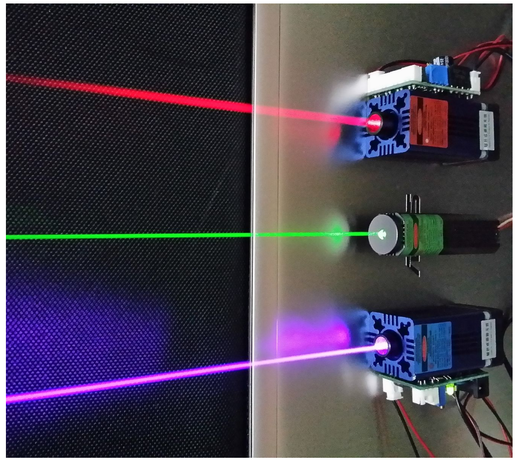
Are there other quantum algorithms with groundbreaking impact?

What is a quantum computer?

“Non-computing” quantum devices

Stimulated emission

- Laser
- Atomic clock, GPS



Tunnelling

- Flash memory
- Scanning tunneling microscope

Magnetic resonance

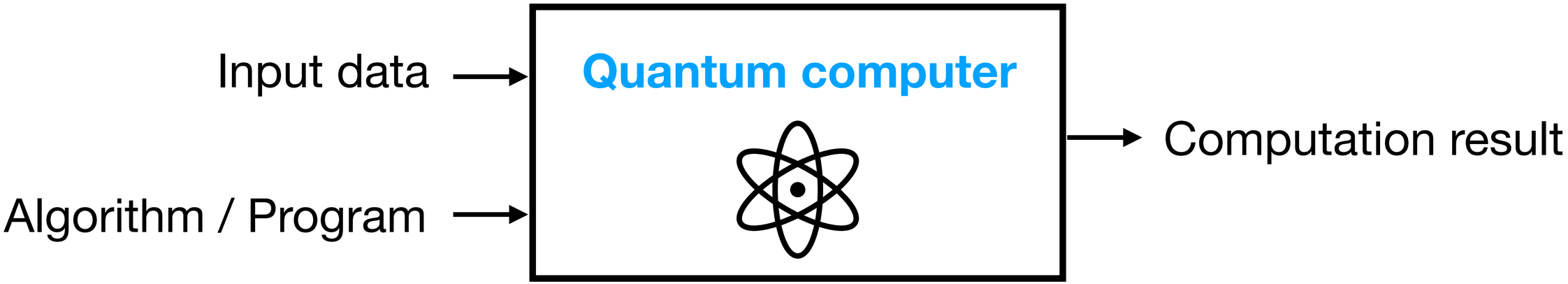
- Magnetic Resonance Imaging
- NMR spectroscopy

Photoelectric & Photovoltaic effect

- Solar panel
- CCD sensor

What is a quantum computer?

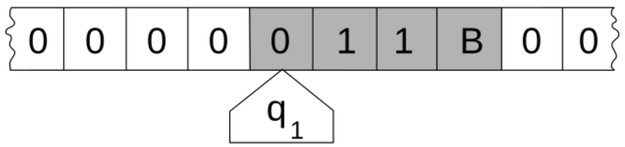
A physical device that exploits the laws of quantum mechanics to perform computations on data



Example of tasks: find integer solutions to $x^2 - 511y^2 = 1$, simulate the FeMoco molecule, find the prime decomposition of $2^{1550019073} - 1$

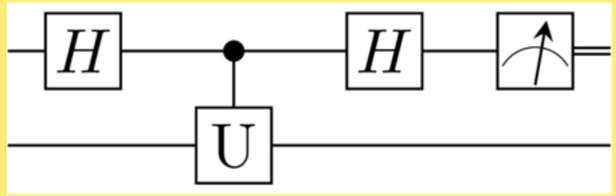
How to (*mathematically*) construct a quantum computer?

Several mathematical models describing how quantum computers are expected to behave:



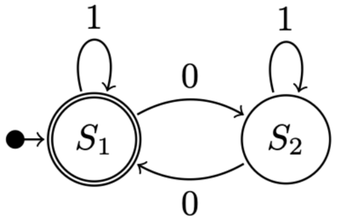
Q. Turing machine

(~1980-85)



Q. circuit

(~1989-93)



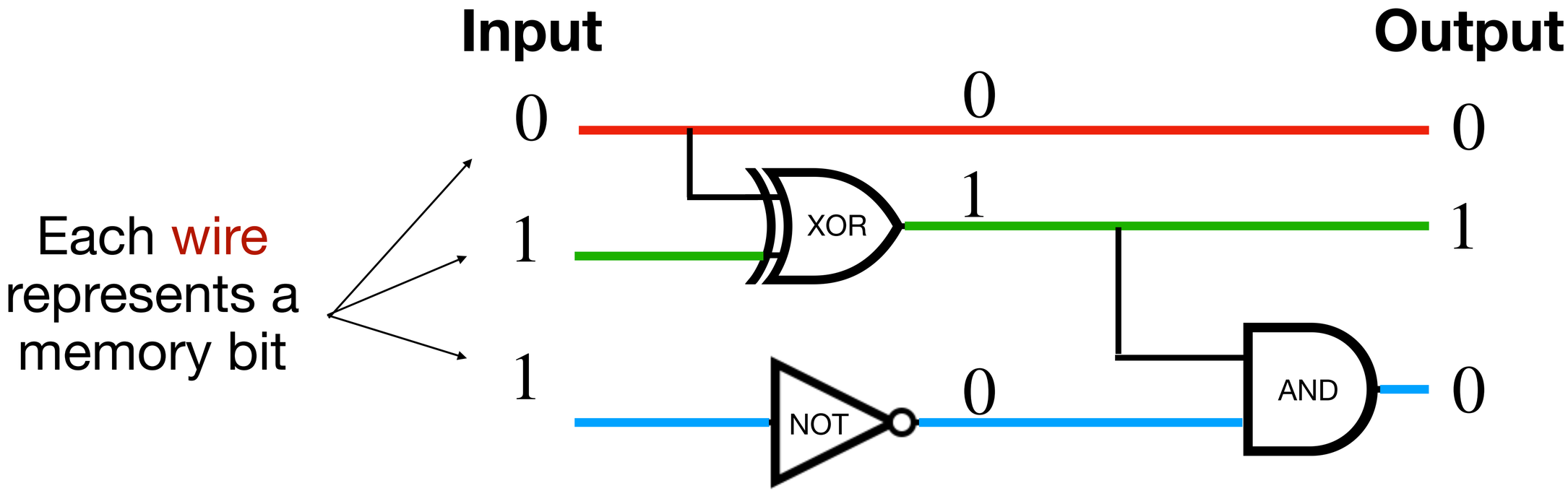
Q. finite automaton

(~1997-2000)

…

Classical computers

A classical computer can be modeled as a sequence of Boolean operations acting on a memory of bits



Quantum computers

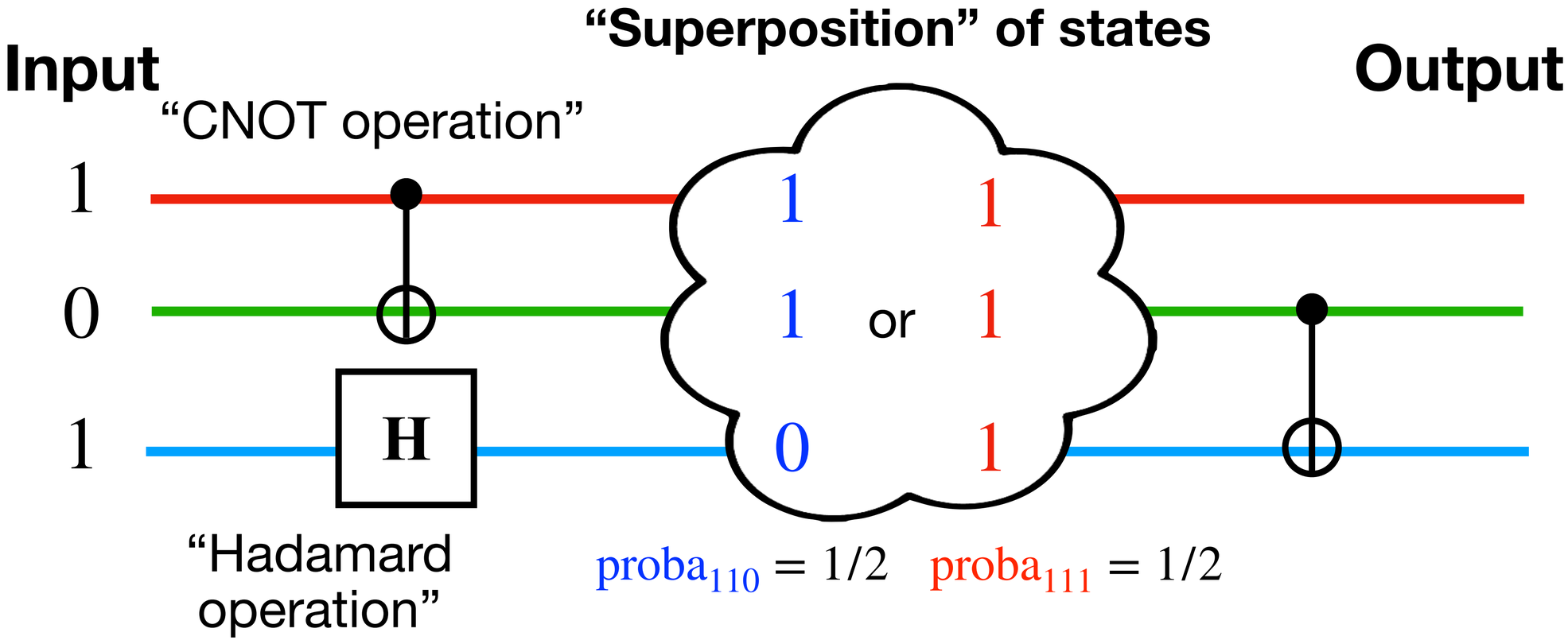
quantum

A ~~classical~~ computer can be modeled as a sequence of

~~Boolean~~ operations acting on a memory of ~~bits~~

unitary

qubits

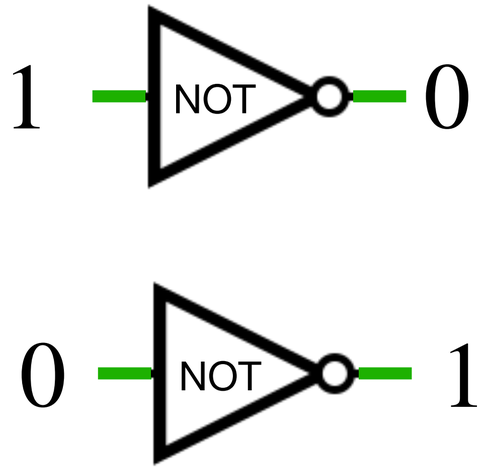


How to (*physically*) construct a quantum computer?

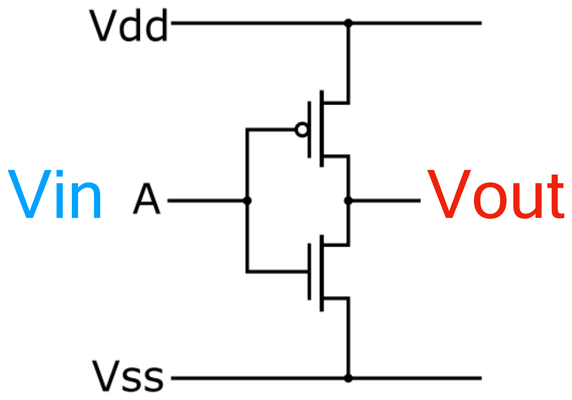
Classical computers

Several technologies (e.g., transistors) can faithfully simulate the classical mathematical models

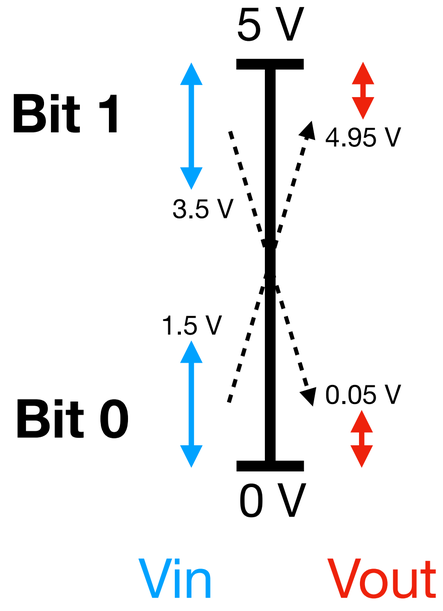
NOT operation



=

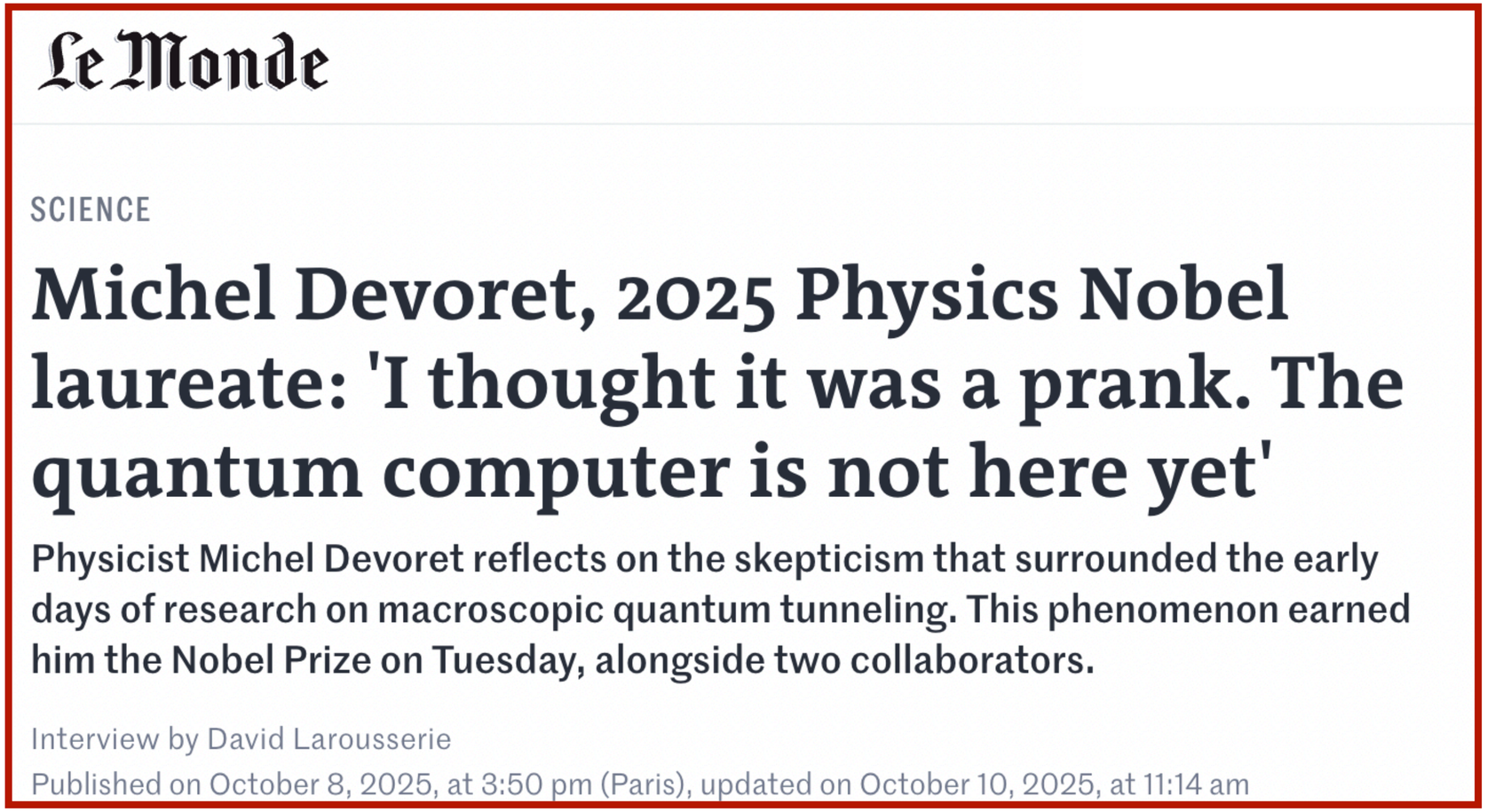


CMOS inverter



Quantum computers

No technology is currently able to implement the quantum mathematical models at large scale



Le Monde

SCIENCE

Michel Devoret, 2025 Physics Nobel laureate: 'I thought it was a prank. The quantum computer is not here yet'

Physicist Michel Devoret reflects on the skepticism that surrounded the early days of research on macroscopic quantum tunneling. This phenomenon earned him the Nobel Prize on Tuesday, alongside two collaborators.

Interview by David Larousserie

Published on October 8, 2025, at 3:50 pm (Paris), updated on October 10, 2025, at 11:14 am

Quantum computers

No technology is currently able to implement the quantum mathematical models at large scale

Some major challenges:

- Imperfections in qubits/gates implementations (noise accumulation)
- Decoherence effects (uncontrolled loss of quantum properties)

… spanning theoretical, experimental, and engineering aspect:

- designing efficient quantum error-correcting codes
- constructing high-quality qubits
- …

Candidates technologies for physical qubits

Superconductors

ALICE & BOB

Google

IBM

amazon

Trapped ions

QUANTINUUM

IONQ

Photons

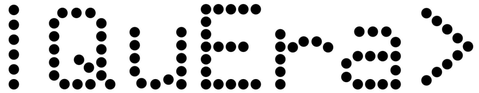
QUANDELA

XANADU

PsiQuantum

Neutral atoms

PASQAL



Silicon spin

quobly

...

When will quantum computers arrive?

Many companies have roadmaps aiming for the first fully functional, moderately large quantum computers by ~2030 … this looks very optimistic

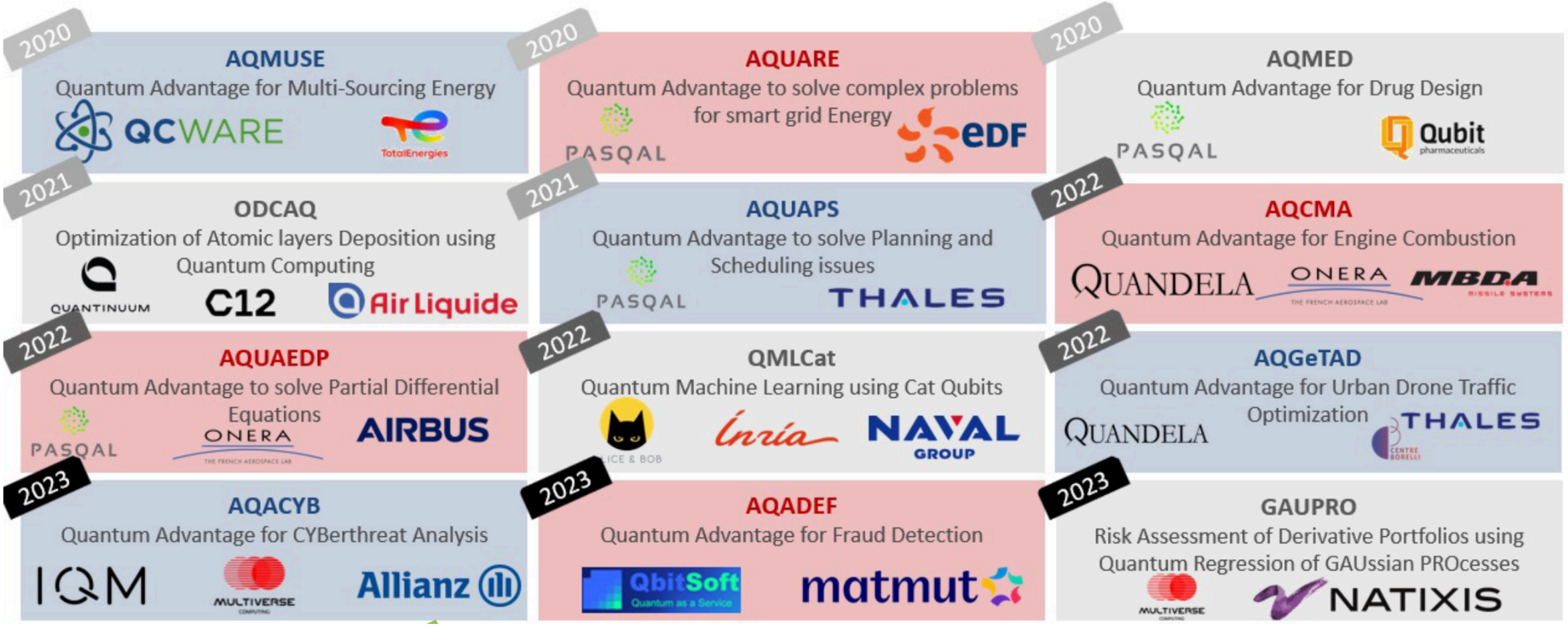
Defense and security agencies warn of a quantum threat within 10-15 years

What we see at the moment:

- Steady progress in the technologies
- Sustained investments by public and private actors
- Push from manufacturers to start selling prototype quantum computers
- Broad industrial interest in potential quantum applications

What can quantum algorithms do?

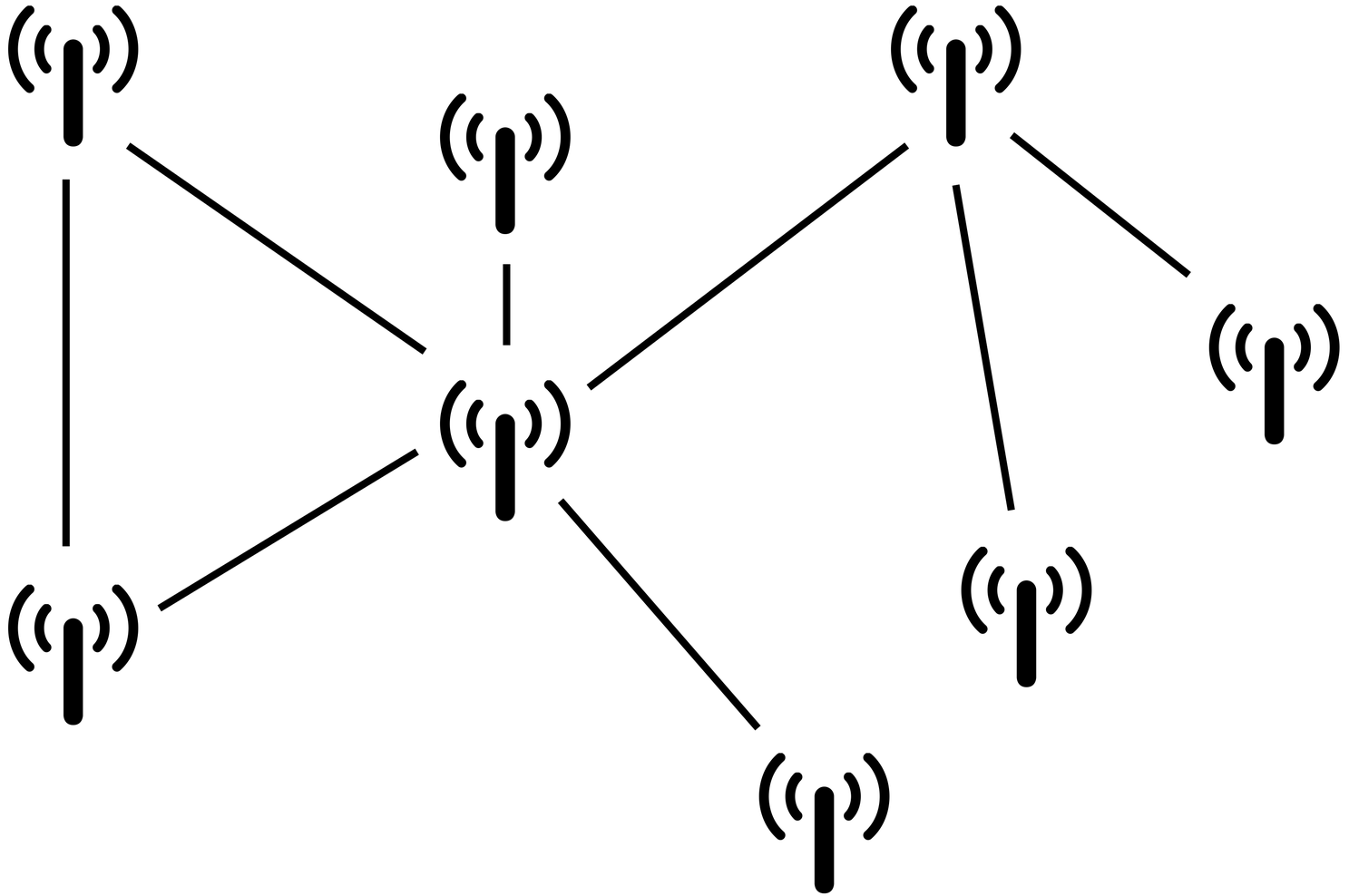
Some exploratory projects (Pack Quantique)



https://teratec.eu/Seminaires/TQCI/2024/Journee_Pack_Quantique_TQCI-240424.html

Similar initiatives: Maisons du quantique, CEMRACS 2025, …

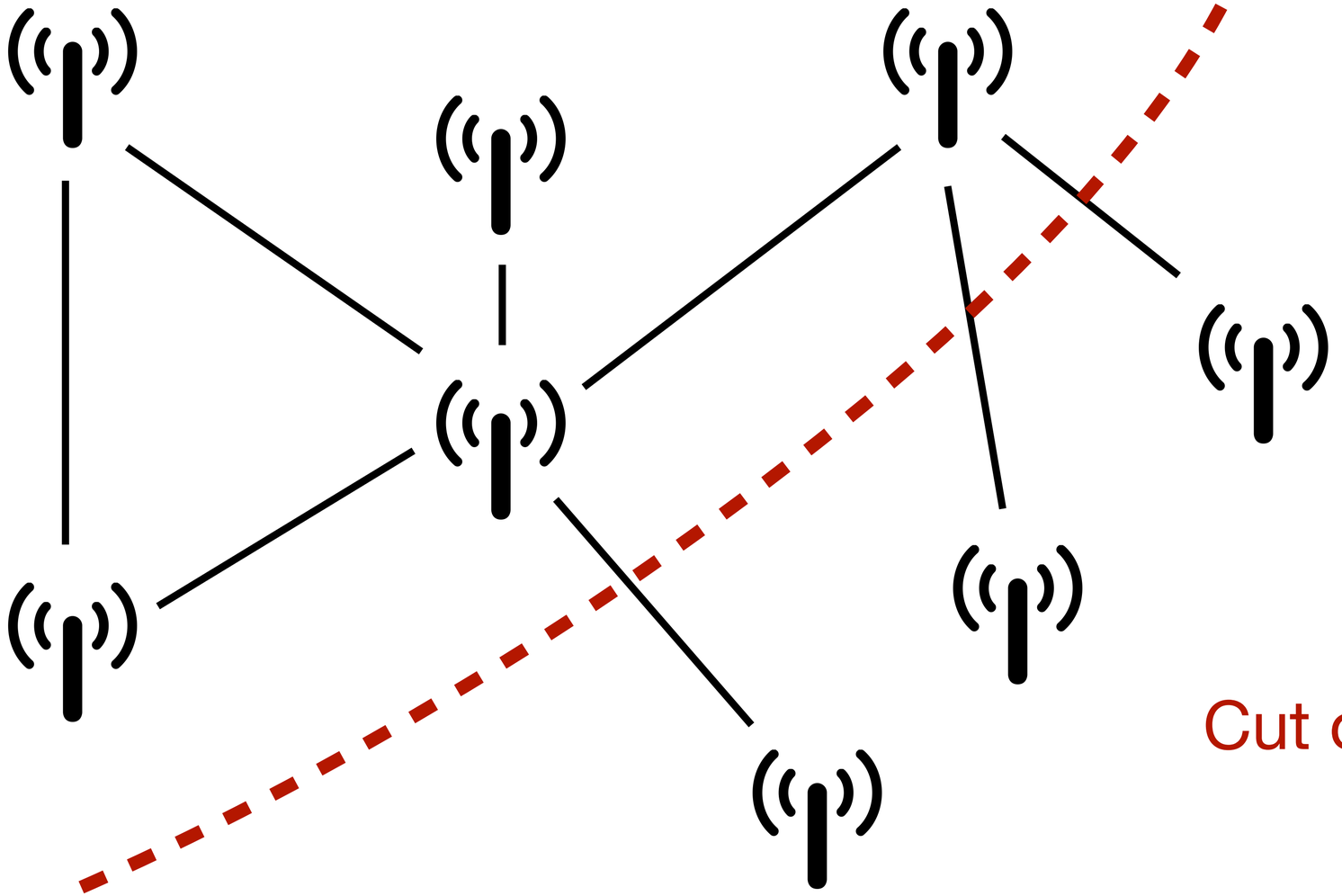
Toy example: Antenna maintenance



Split antennas into two groups maximizing connectivity between them

(Max-Cut problem)

Toy example: Antenna maintenance

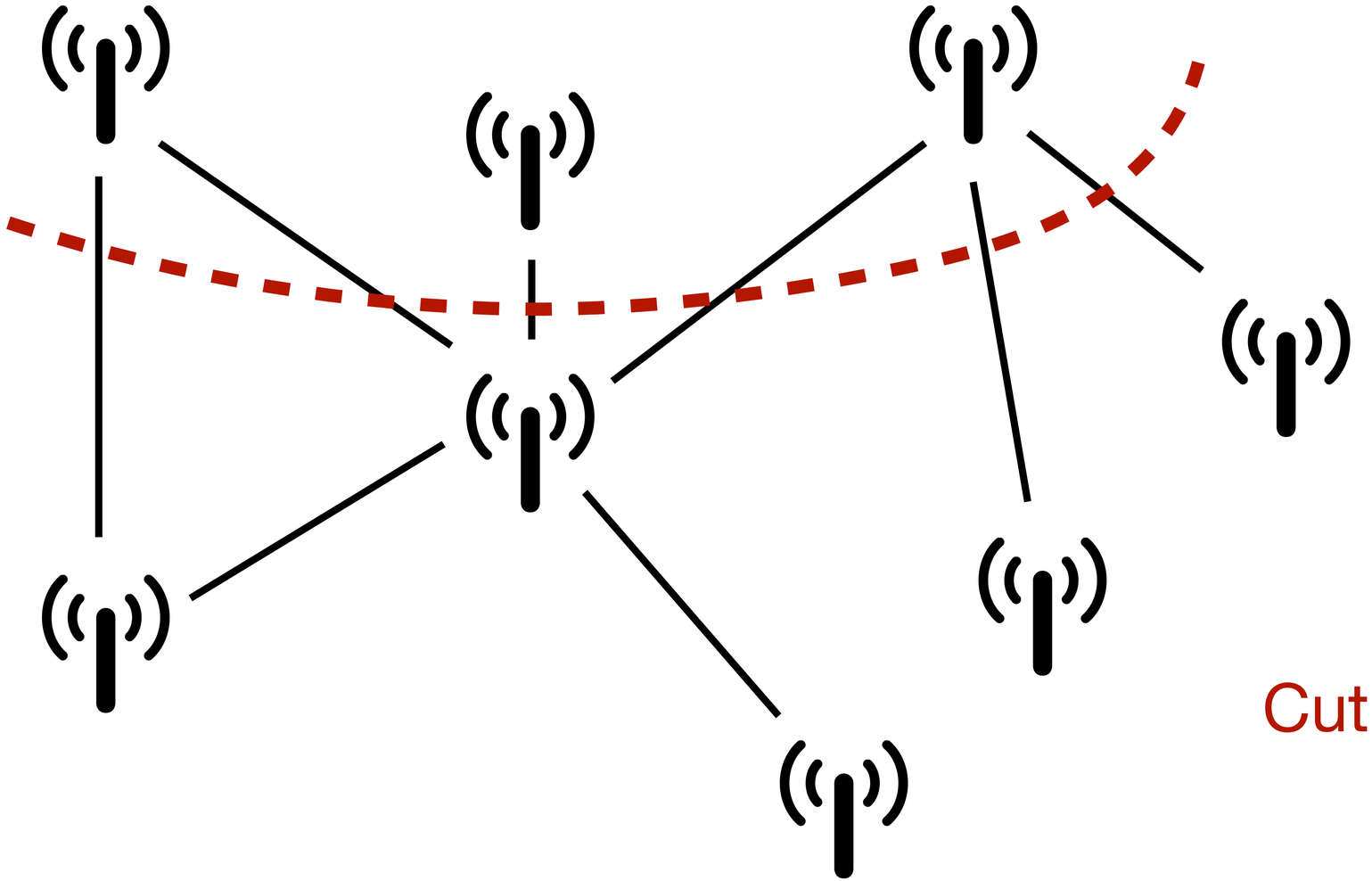


Split antennas into two groups maximizing connectivity between them

(Max-Cut problem)

Cut of value 3

Toy example: Antenna maintenance



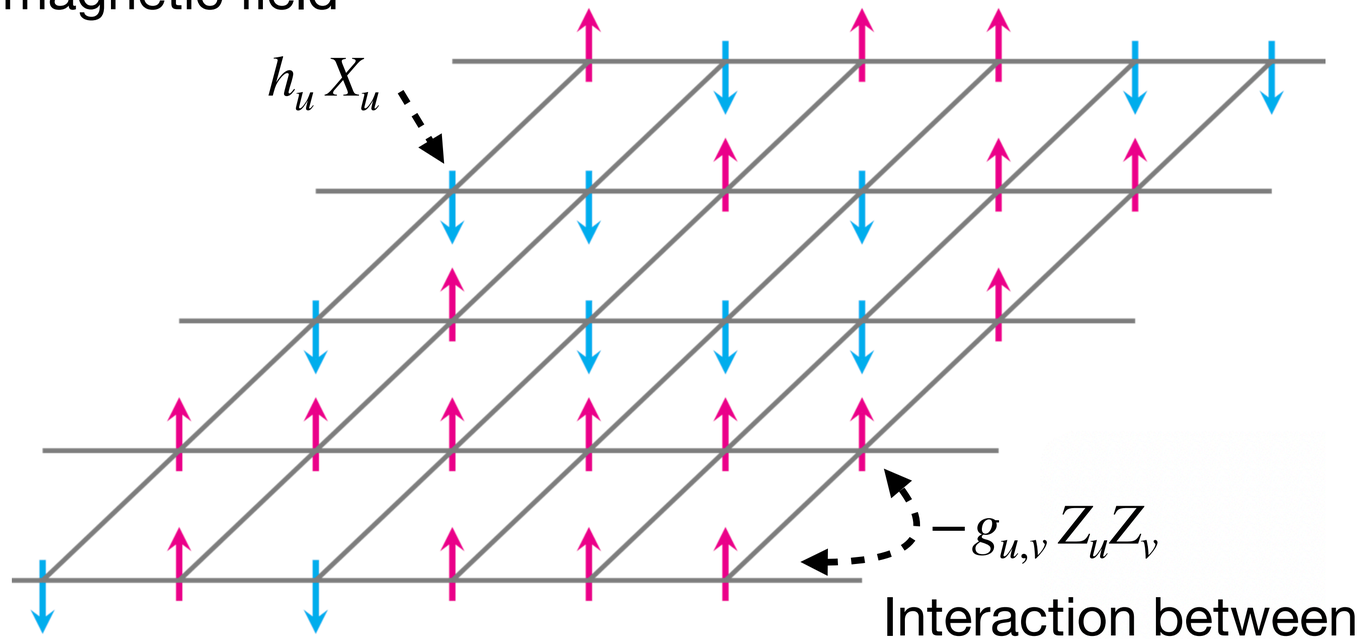
Split antennas into two groups maximizing connectivity between them

(Max-Cut problem)

Cut of value 6
(best)

Physical interpretation: Ising model

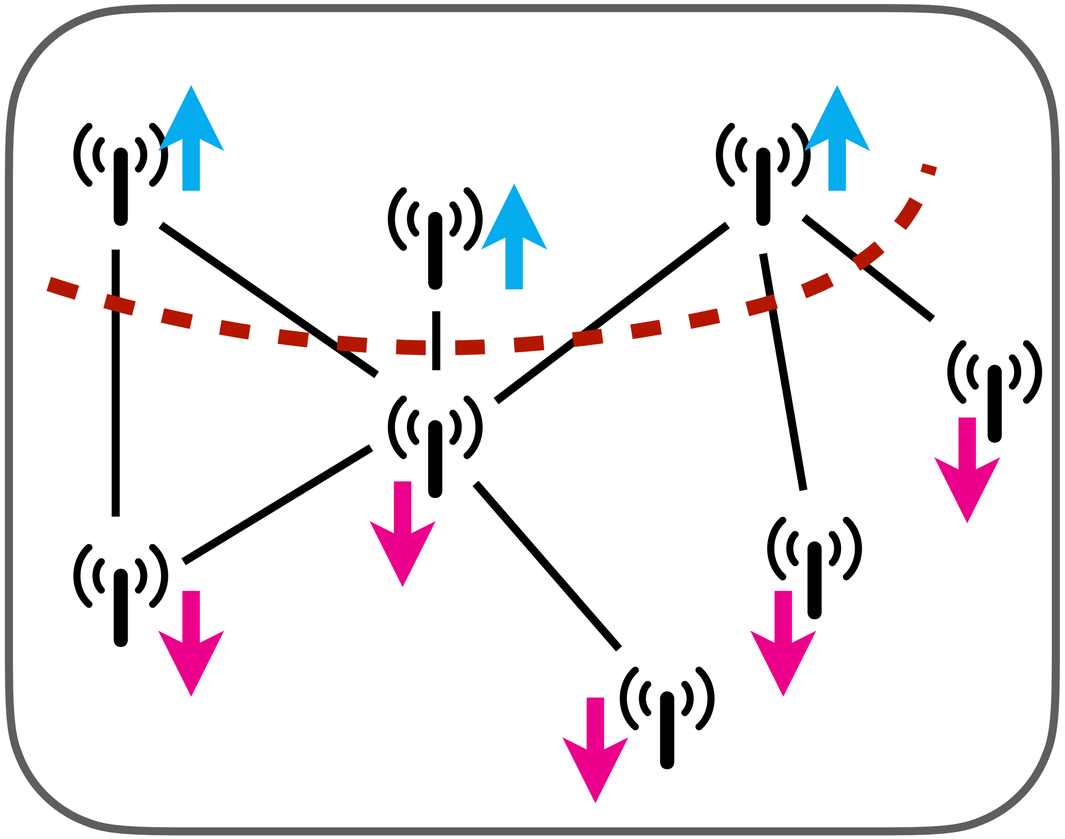
Transverse magnetic field



Interaction between neighboring particles

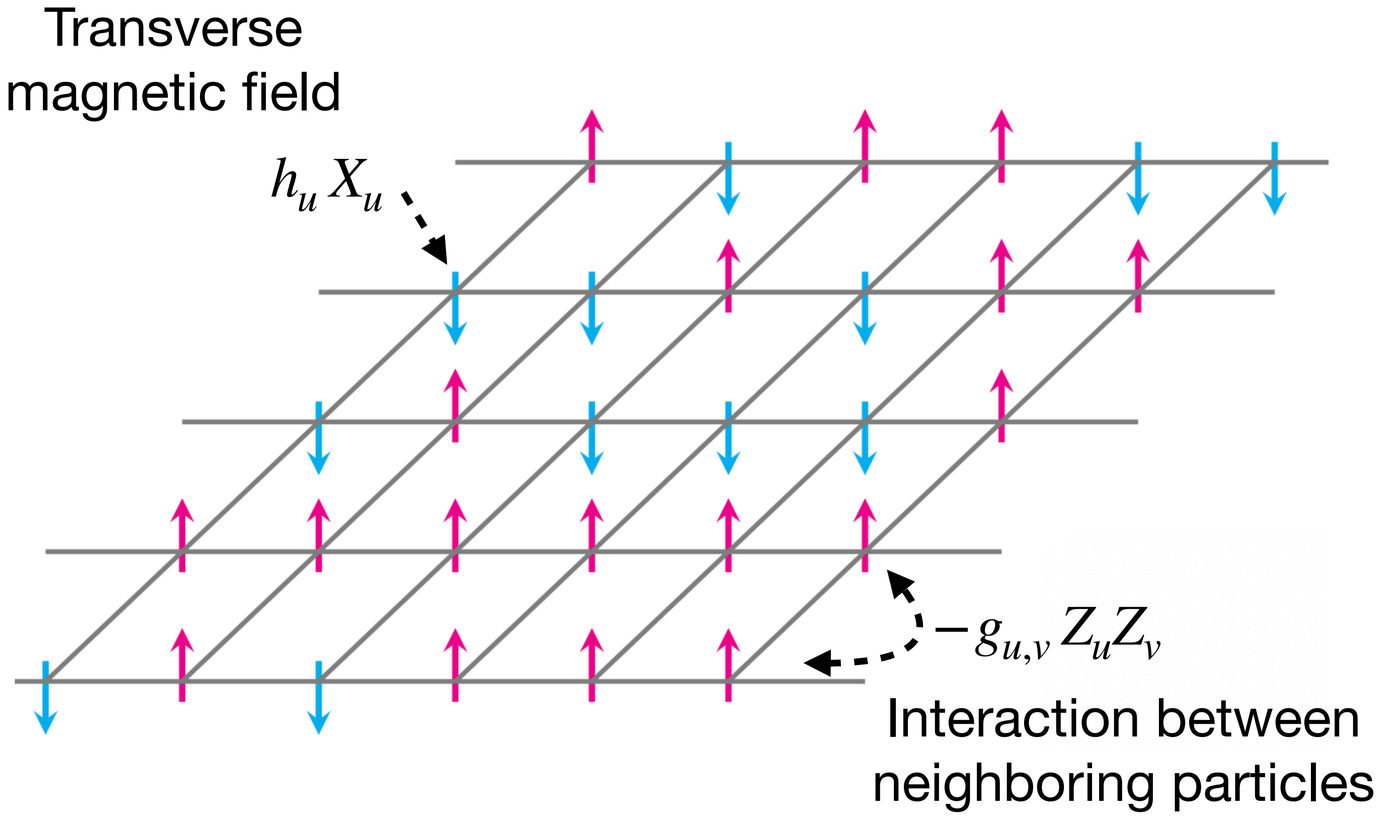
$$H = \sum_{(u,v)} h_u X_u - g_{u,v} Z_u Z_v$$

Pauli matrices



Optimal solution =
Minimum eigenvalue of *H*

Physical interpretation: Ising model



$$H = \sum_{(u,v)} h_u X_u - g_{u,v} Z_u Z_v$$

Pauli matrices

Quantum algorithms for minimum eigenvalue computation

Faster ?

- Phase estimation
- Adiabatic algorithm
- QAOA
- Variational algorithms

...

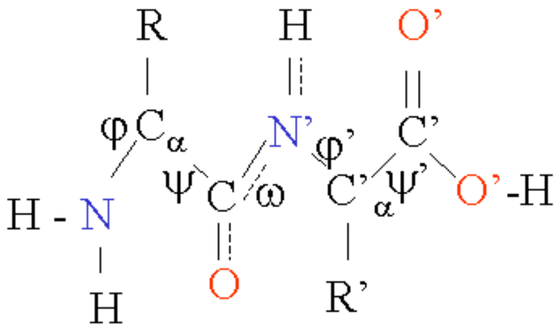
Accurate ?

Optimal solution =
Minimum eigenvalue of *H*

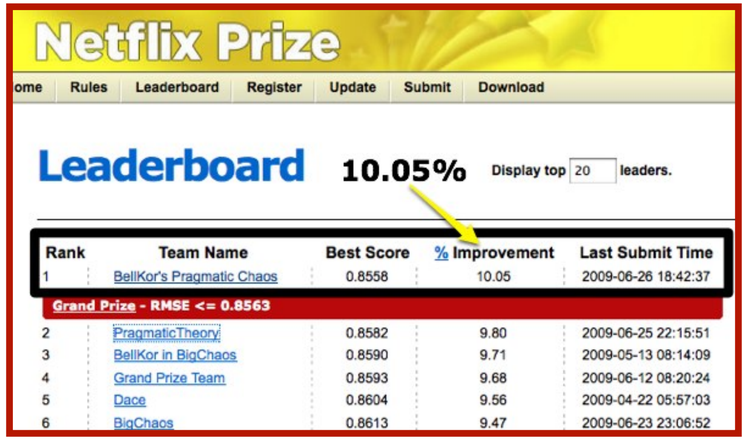
A last message:

Advances in quantum algorithms go hand in hand with advances in classical algorithms

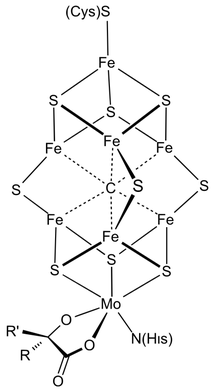
Protein structure prediction



Recommandation systems



Electronic structure simulation



Quantum optimization algorithms ↕ Deep learning (AlphaFold…)

Quantum HHL algorithm ↕ “Dequantized” algorithms

Quantum phase estimation ↕ Tensor networks, coupled cluster…

Further perspectives

A brief history of quantum vs classical computational advantage

Ryan LaRose

In this review article we summarize all experiments claiming quantum computational advantage to date. Our review highlights challenges, loopholes, and refutations appearing in subsequent work to provide a complete picture of the current statuses of these experiments. In addition, we also discuss theoretical computational advantage in example problems such as approximate optimization and recommendation systems. Finally, we review recent experiments in quantum error correction -- the biggest frontier to reach experimental quantum advantage in Shor's algorithm.

https://arxiv.org/abs/2412.14703

The vast world of quantum advantage

Hsin-Yuan Huang, Soonwon Choi, Jarrod R. McClean, John Preskill

The quest to identify quantum advantages lies at the heart of quantum technology. While quantum devices promise extraordinary capabilities, from exponential computational speedups to unprecedented measurement precision, distinguishing genuine advantages from mere illusions remains a formidable challenge. In this endeavor, quantum theorists are like prophets attempting to foretell the future, yet the boundary between visionary insight and unfounded fantasy is perilously thin. In this perspective, we examine our mathematical tools for navigating the vast world of quantum advantages across computation, learning, sensing, and communication. We explore five keystone properties: predictability, typicality, robustness, verifiability, and usefulness that define an ideal quantum advantage, and envision what new quantum advantages could arise in a future with ubiquitous quantum technology. We prove that some quantum advantages are inherently unpredictable using classical resources alone, suggesting a landscape far richer than what we can currently foresee. While mathematical rigor remains our indispensable guide, the ultimate power of quantum technologies may emerge from advantages we cannot yet conceive.

https://arxiv.org/abs/2508.05720

Quantum algorithms: A survey of applications and end-to-end complexities

Alexander M. Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, Chi-Fang Chen, András Gilyén, Connor T. Hann, Michael J. Kastoryano, Emil T. Khabiboulline, Aleksander Kubica, Grant Salton, Samson Wang, Fernando G. S. L. Brandão

The anticipated applications of quantum computers span across science and industry, ranging from quantum chemistry and many-body physics to optimization, finance, and machine learning. Proposed quantum solutions in these areas typically combine multiple quantum algorithmic primitives into an overall quantum algorithm, which must then incorporate the methods of quantum error correction and fault tolerance to be implemented correctly on quantum hardware. As such, it can be difficult to assess how much a particular application benefits from quantum computing, as the various approaches are often sensitive to intricate technical details about the underlying primitives and their complexities. Here we present a survey of several potential application areas of quantum algorithms and their underlying algorithmic primitives, carefully considering technical caveats and subtleties. We outline the challenges and opportunities in each area in an "end-to-end" fashion by clearly defining the problem being solved alongside the input-output model, instantiating all "oracles," and spelling out all hidden costs. We also compare quantum solutions against state-of-the-art classical methods and complexity-theoretic limitations to evaluate possible quantum speedups.

https://arxiv.org/abs/2310.03011

Slides: https://yassine-hamoudi.github.io/files/slides/JIQToulouse.pdf

Image credit: Wikimedia Commons