Quantum refresh & intro

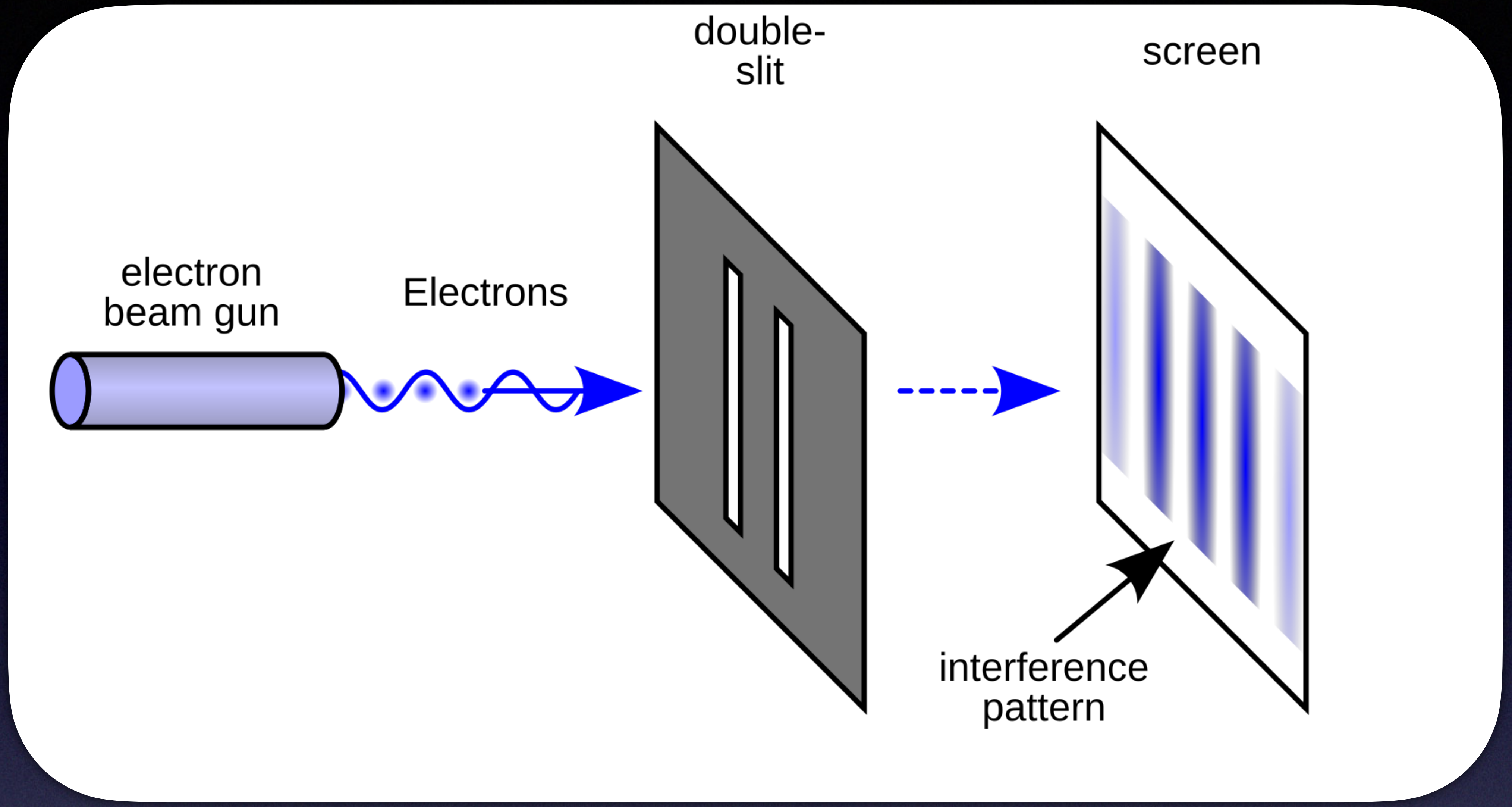
a short intro/reminder of properties and peculiarities
(hopefully) useful to understand the Quantum Computing

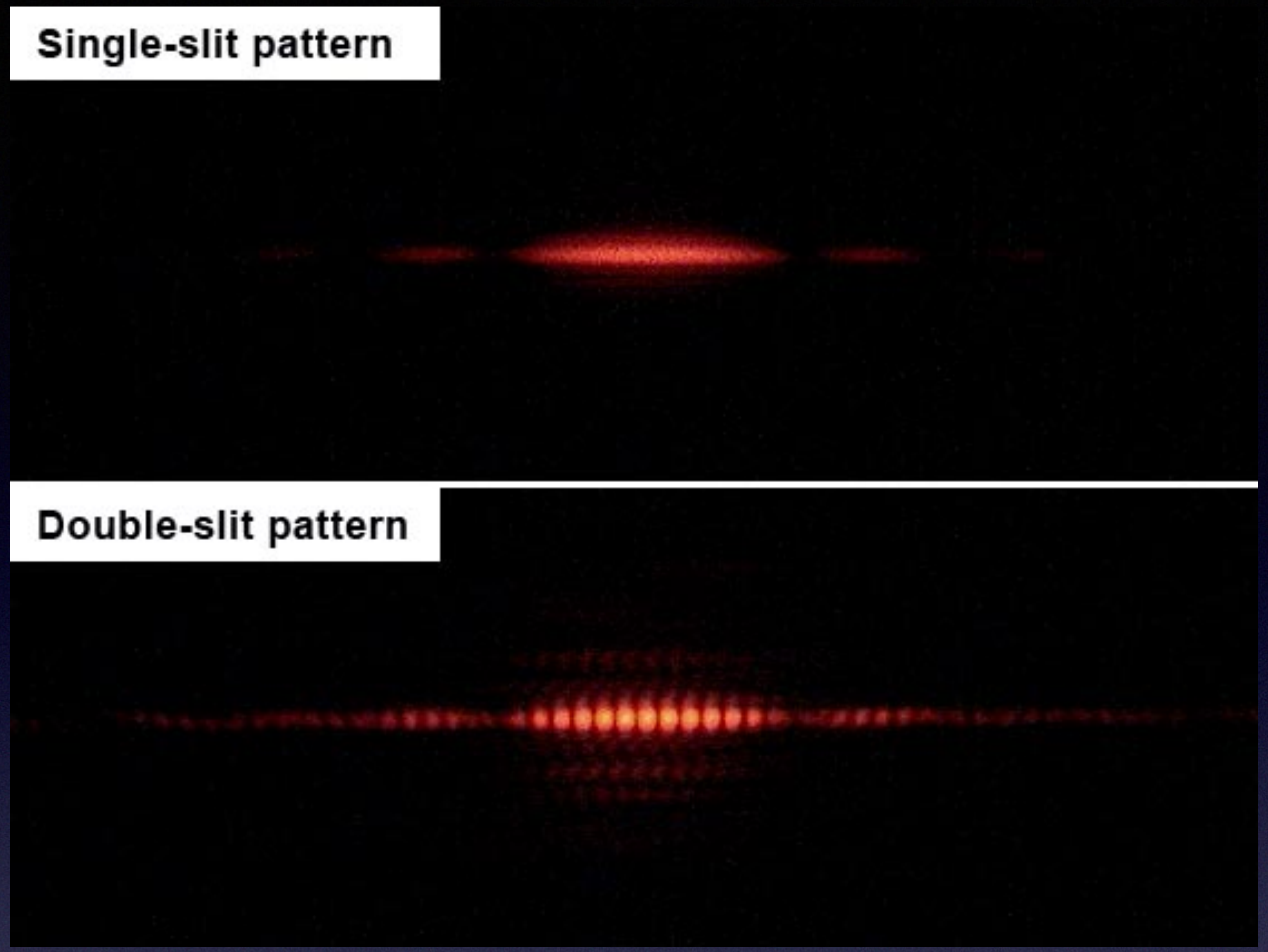
R. Scaramella - Trieste March 2026 - INAF USC-C

Overview

- Quantum: why and how
- wave/particle behaviour
- interference
- wave function, probabilistic interpretation
- superposition, Qbit, entanglement, EPR & Bell inequalities
- quantum computing: notation and circuits vs hardware
- list of some applications in astronomy/cosmology

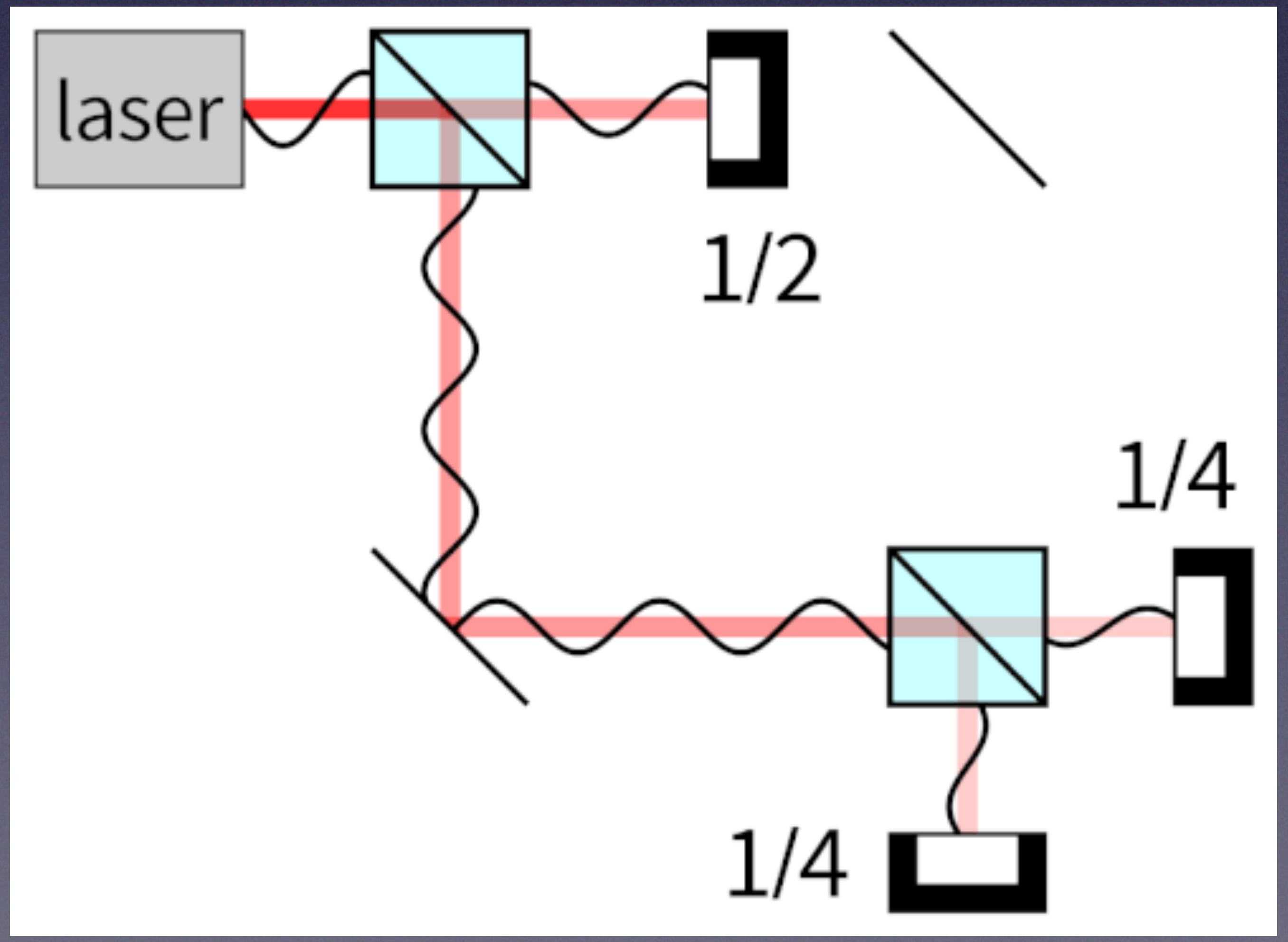
Famous double slit experiment





This happens also for single particles! (one at a time)

Light in Mach–Zehnder interferometer produces interference (wave-like behavior) even when being detected one photon at a time (particle-like behavior).



Copenhagen probabilistic interpretation

[relational interpretation, many worlds, De Broglie--Bohm]

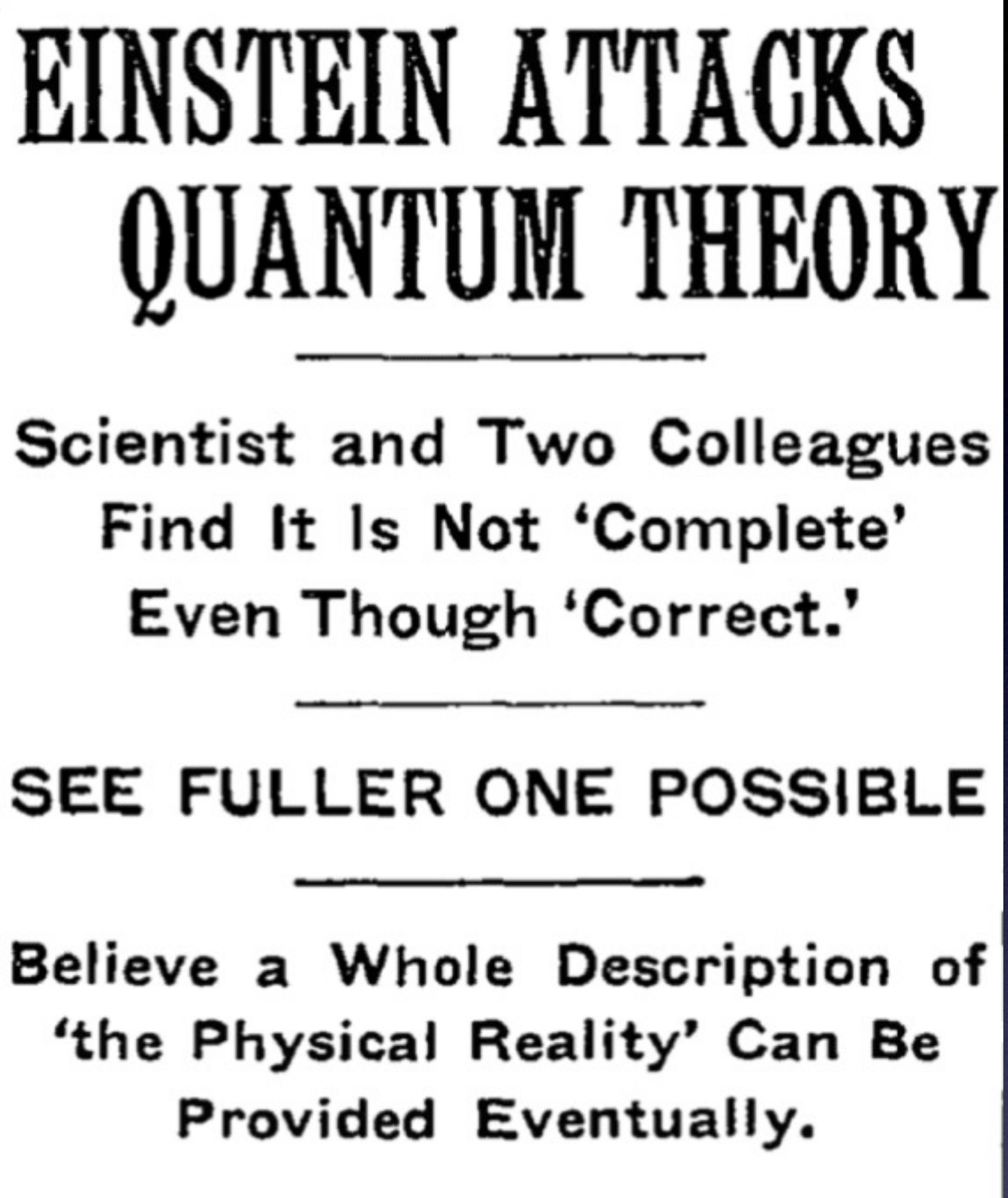
Quantum pills

Quantum mechanics is the theory that describes the behavior of microscopic systems, such as photons, electrons, atoms, molecules, etc.

Nobody understands quantum mechanics!

"No, you're not going to be able to understand it.... You see, my physics students don't understand it either. That is because I don't understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with an experiment. So I hope that you can accept Nature as She is – absurd"
--Richard Feynman

Max Planck, Albert Einstein,
Niels Bohr, Louis de Broglie,
Max Born, Paul Dirac,
Werner Heisenberg, Wolfgang Pauli,
Erwin Schrödinger, Richard Feynman



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Entanglement & Bell's inequality

Richard Feynman

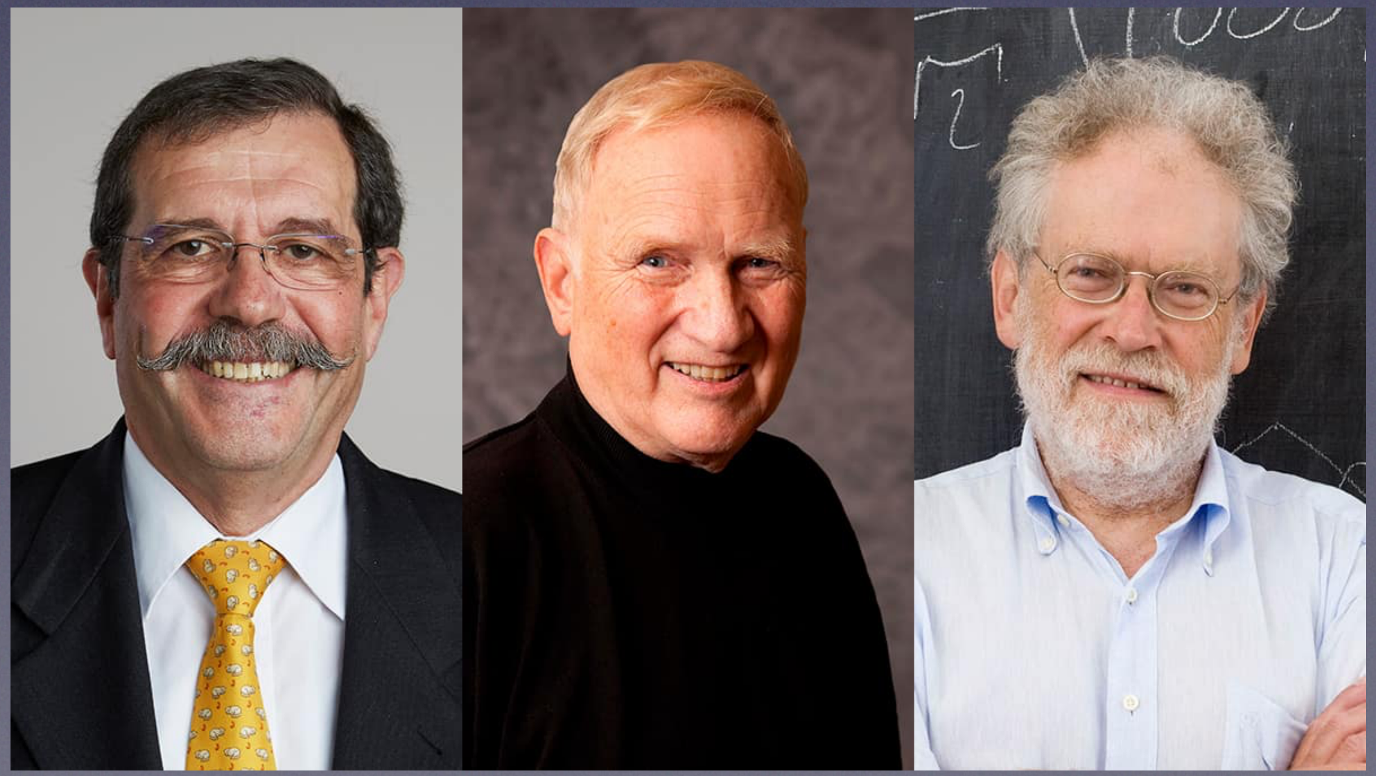
"There's Plenty of Room at the Bottom" (1959)

"When we get to the very, very small world – say circuits of sever
atoms – we have a lot of new things that would happen that represent **completely new opportunities for design**.
Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics..."

6

Alain Aspect, John Clauser, and Anton Zeilinger, the winners of the 2022 Nobel Prize in Physics.

Entanglement



John Clarke, Michel Devoret and John Martinis win the 2025 Nobel Prize for Physics

Macro quantum

"The basis of quantum computing relies to quite an extent on our discovery."

Quantum states, represented by Dirac's ket, $|\psi\rangle$, evolve in time according to the Schrödinger equation:

$$\frac{d|\psi\rangle}{dt} = -\left(\frac{i}{\hbar}\right) \hat{H}(|\psi\rangle)$$

This implies that time evolution is described by unitary transformations: $|\psi\rangle \rightarrow \hat{U}|\psi\rangle$, with $\hat{U} = \hat{U}^\dagger$ is an unitary operator (matrix), $\hat{U}^\dagger = \left(\hat{U}\right)^{-1}$ where $|\psi\rangle$ is the quantum state (wavefunction) and H is Hamiltonian. $\hat{U}^\dagger$ is the hermitian conjugate (array is transposed and complex conjugated), $\hat{U}^\dagger = \left(\hat{U}^T\right)^* = \left(\hat{U}^*\right)^T$

$$\frac{d\hat{U}(t)}{dt} = -\frac{i}{\hbar}\hat{H}(t)\,\hat{U}(t)$$

This theory, which has been extensively tested by experiments, **is probabilistic in nature.**
The outcomes of measurements on quantum systems are not deterministic.
Between measurements, quantum systems evolve according to linear equations (the Schrödinger equation).
This means that solutions to the equations obey a superposition principle: **linear combinations of solutions are still solutions**.

Quantum Bit → Qubit

- Since quantum systems evolve according to linear equations (the Schrödinger equation), **linear combinations of solutions are also solutions**.
- So, for the state of a qubit $|0\rangle$ and $|1\rangle$, its superposition also describes a state
- The **general form of a qubit state** can be represented by: $\alpha_0|0\rangle + \alpha_1|1\rangle$

where α_0 and α_1 are **complex numbers that specify the probability amplitudes** of the corresponding states.

- $|\alpha_0|^2$ gives the probability that you will find the qubit in the "off" $|0\rangle$ state; $|\alpha_1|^2$ gives the probability that you will find the qubit in the "on" $|1\rangle$ state.
- Normalization condition: $|\alpha_0|^2 + |\alpha_1|^2 = 1$

$$|\psi\rangle = e^{i\gamma}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right]$$

So electrons with spin 1/2 have two states. However, recall that the photon has 1 spin but only two states of polarisation (helicity) because it moves at c.

Typical notation

Two level system eigenstates: $|\psi\rangle = |0\rangle$ **or** $|\psi\rangle = |1\rangle$ **(spin down or up)**

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

$$|\psi\rangle = e^{i\gamma} \left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|1\rangle \right)$$

$$\langle\psi|\psi\rangle = |\psi|^2 = 1$$

density operator $\rho = \frac{1}{2}\left(I + \vec{a}\cdot\vec{\sigma}\right)$ Pauli matrices $\vec{\sigma}$

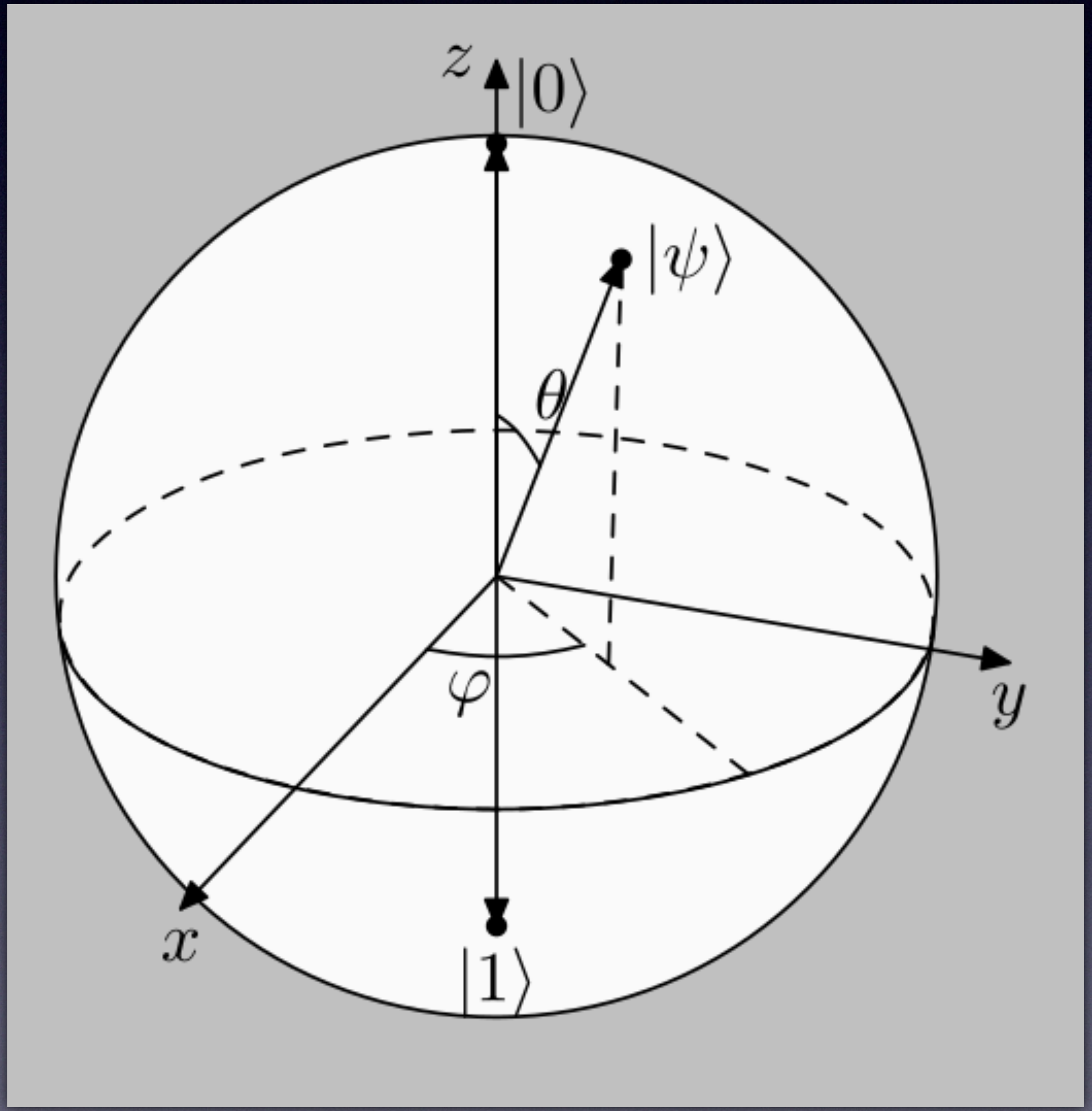
$$\rho = \frac{1}{2}\left(I + \vec{a}\cdot\vec{\sigma}\right) \qquad \rho = \frac{1}{2}\begin{pmatrix} 1 + a_z & a_x - ia_y \\ a_x + ia_y & 1 - a_z \end{pmatrix}$$

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + w & u - iv \\ u + iv & 1 - w \end{pmatrix}$$

Bloch sphere

$$\vec{a} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

$$\vec{a} = (a_x, a_y, a_z) = (u, v, w)$$



Rotation along versor $\hat{n}$ $R_{\hat{n}}(\theta) = exp\left(-i\theta\hat{n}\cdot\vec{\sigma}/2\right)$

$\langle\,|$ =bra $|\,\rangle$=ket

$\langle\,|\,\rangle$=number

$\sum_n |n\rangle\langle n|$ =basis

1 qbit

$$|0\rangle = 1|0\rangle + 0|1\rangle \rightarrow \begin{bmatrix}1\\0\end{bmatrix}$$

$$|1\rangle = 0|0\rangle + 1|1\rangle \rightarrow \begin{bmatrix}0\\1\end{bmatrix}$$

$$\langle 0| = 1\langle 0| + 0\langle 1| \rightarrow \begin{bmatrix}1 & 0\end{bmatrix}$$

$$\langle 1| = 0\langle 0| + 1\langle 1| \rightarrow \begin{bmatrix}0 & 1\end{bmatrix}$$

$$|v\rangle = v_0|0\rangle + v_1|1\rangle = v_0\begin{bmatrix}1\\0\end{bmatrix} + v_1\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}v_0\\v_1\end{bmatrix}$$

2 qbits

$$|a\rangle = \begin{bmatrix}a_0\\a_1\end{bmatrix} \quad \text{and} \quad |b\rangle = \begin{bmatrix}b_0\\b_1\end{bmatrix}$$

$$|x\rangle = |a\rangle \otimes |b\rangle = |ab\rangle$$

tensor product

$$|x\rangle = \begin{bmatrix} a_0 * \begin{bmatrix}b_0\\b_1\end{bmatrix} \\ a_1 * \begin{bmatrix}b_0\\b_1\end{bmatrix} \end{bmatrix} = \begin{bmatrix}a_0b_0\\a_0b_1\\a_1b_0\\a_1b_1\end{bmatrix} = \begin{bmatrix}x_0\\x_1\\x_2\\x_3\end{bmatrix}$$

$$|x\rangle = a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

$$|x\rangle = x_0|00\rangle + x_1|01\rangle + x_2|10\rangle + x_3|11\rangle$$

$$|a_0b_0|^2 + |a_0b_1|^2 + |a_1b_0|^2 + |a_1b_1|^2 = 1$$

3 qbits

$$|y\rangle = |ab\rangle \otimes |c\rangle = |abc\rangle$$

$$|c\rangle = \begin{bmatrix}c_0\\c_1\end{bmatrix}$$

$$|y\rangle = \begin{bmatrix} a_0b_0 * \begin{bmatrix}c0\\c1\end{bmatrix} \\ a_0b_1 * \begin{bmatrix}c0\\c1\end{bmatrix} \\ a_1b_0 * \begin{bmatrix}c0\\c1\end{bmatrix} \\ a_1b_1 * \begin{bmatrix}c0\\c1\end{bmatrix} \end{bmatrix} = \begin{bmatrix}a_0b_oc_0\\a_0b_oc_1\\a_0b_1c_0\\a_0b_1c_1\\a_1b_oc_0\\a_1b_oc_1\\a_1b_1c_0\\a_1b_1c_1\end{bmatrix} = \begin{bmatrix}y_0\\y_1\\y_2\\y_3\\y_4\\y_5\\y_6\\y_7\end{bmatrix}$$

2^N **coordinates**

Classical Bit vs. Quantum Bit

CLASSICAL BIT:

- can be in two distinct states, 0 and 1
- can be measured completely
- are not changed by measurement
- can be copied
- can be erased

QUANTUM BIT:

- can be in state $|0\rangle$ or in state $|1\rangle$ or in any other state that is a linear combination of the two states
- can be measured partially with given probability
- are changed by measurement
- cannot be copied
- cannot be erased

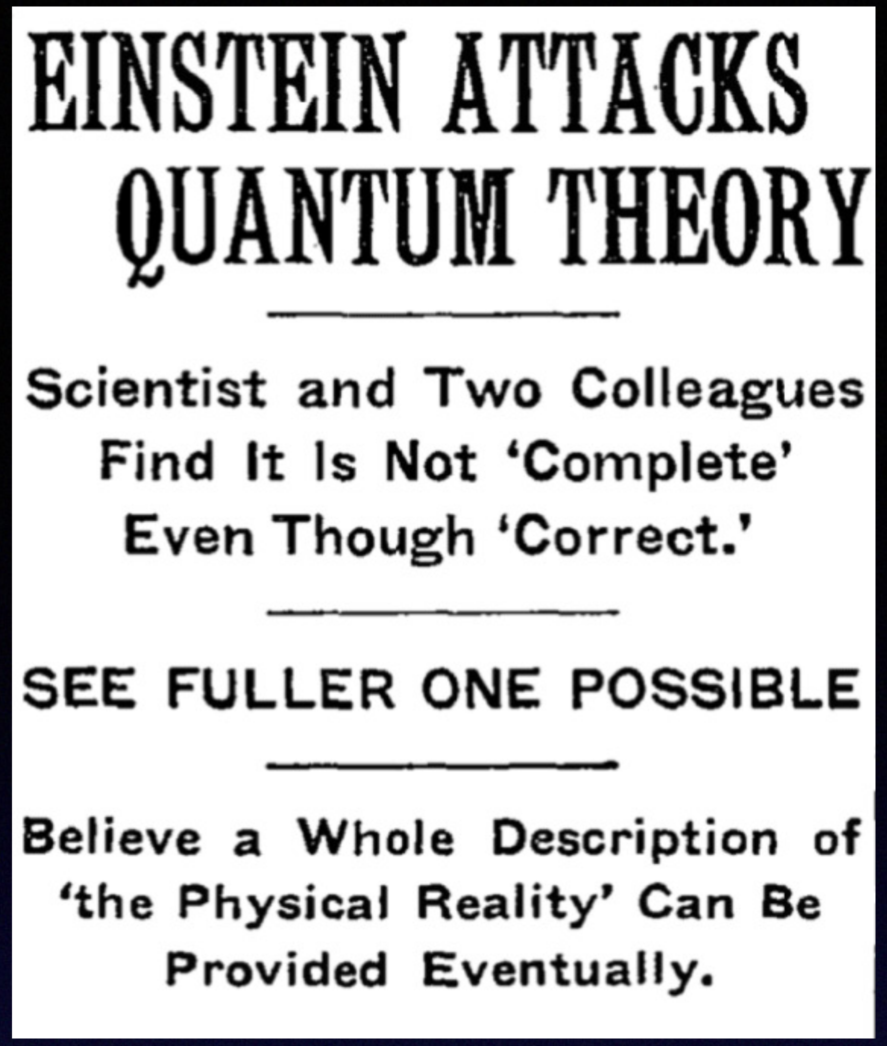
What is a quantum computer?

➢ Classical Computer: a computer that uses voltages flowing through circuits and gates, which can be controlled and manipulated entirely by classical mechanics.

➢ Quantum Computer: a computer that uses laws of quantum mechanics to perform massively parallel computing through superposition, entanglement, and decoherence

Entanglement and some headaches

Einstein–Podolsky–Rosen (EPR) paradox


EINSTEIN ATTACKS QUANTUM THEORY

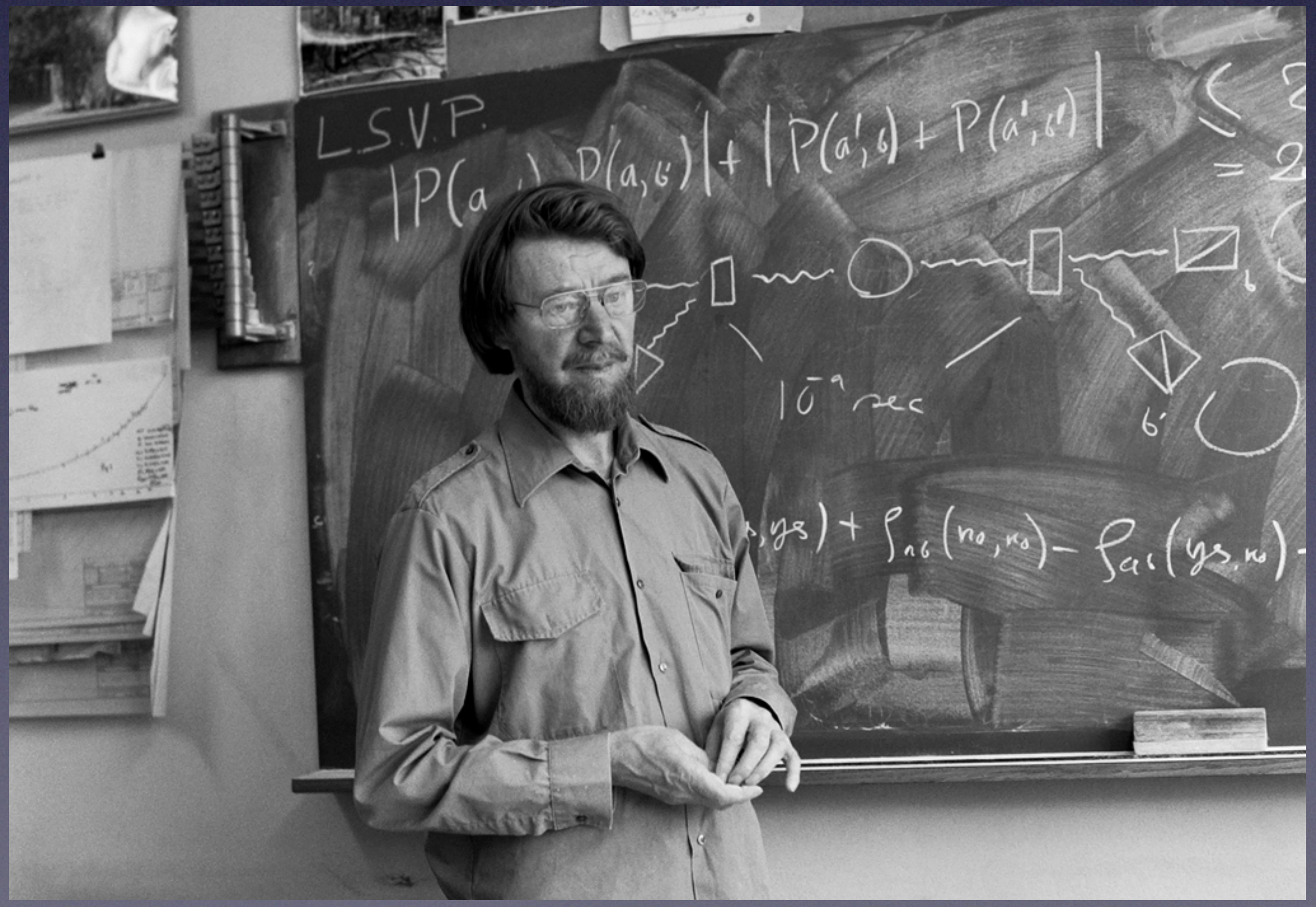
Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

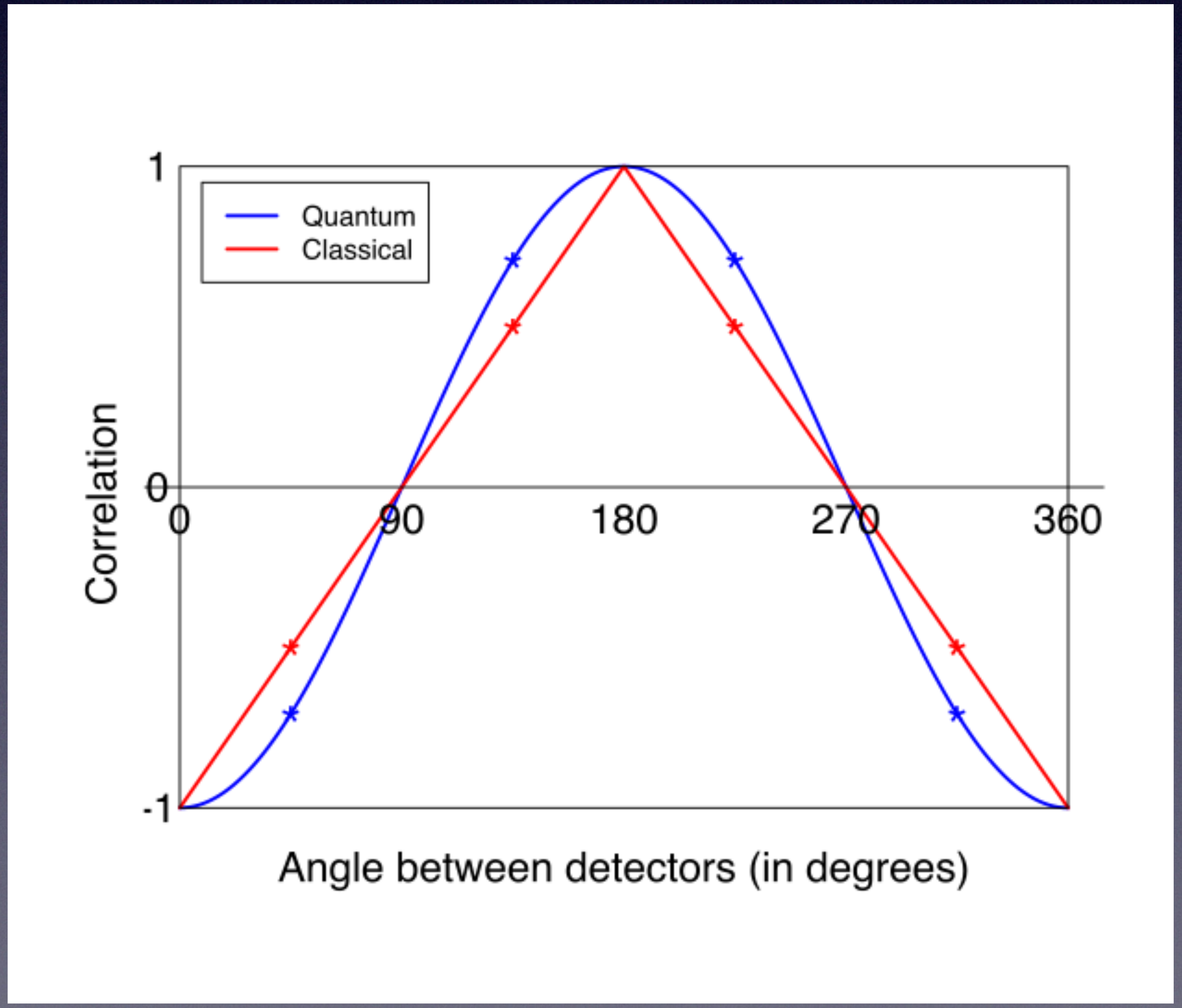
Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

(in)famous *"spooky action at distance"*
i.e. non-locality

Do local "*hidden variables*" exist/are required?



1964. Bell inequalities, or sometimes, Bell-type inequalities. Bell's theorem shows that no theory of local realism such as a local hidden variables theory can account for the correlations between entangled electrons predicted by quantum mechanics.



Entanglement:

a physical state of two (or more) "particles" which appear to have correlated properties independently of their mutual space distance: there is a restricted space of possible outcomes such that if, e.g., one of two entangled particles is *measured* to have spin up ,$|0\rangle$, then the other will always have spin down, $|1\rangle$, The opposite is true: if the first is measured to have spin down, $|1\rangle$ then the other will always have spin up ,$|0\rangle$ (collapse of wave function)

Entanglement is fragile: any interactions with other particles/environment can destroy it (decoherence). A measure of any particle destroys it.

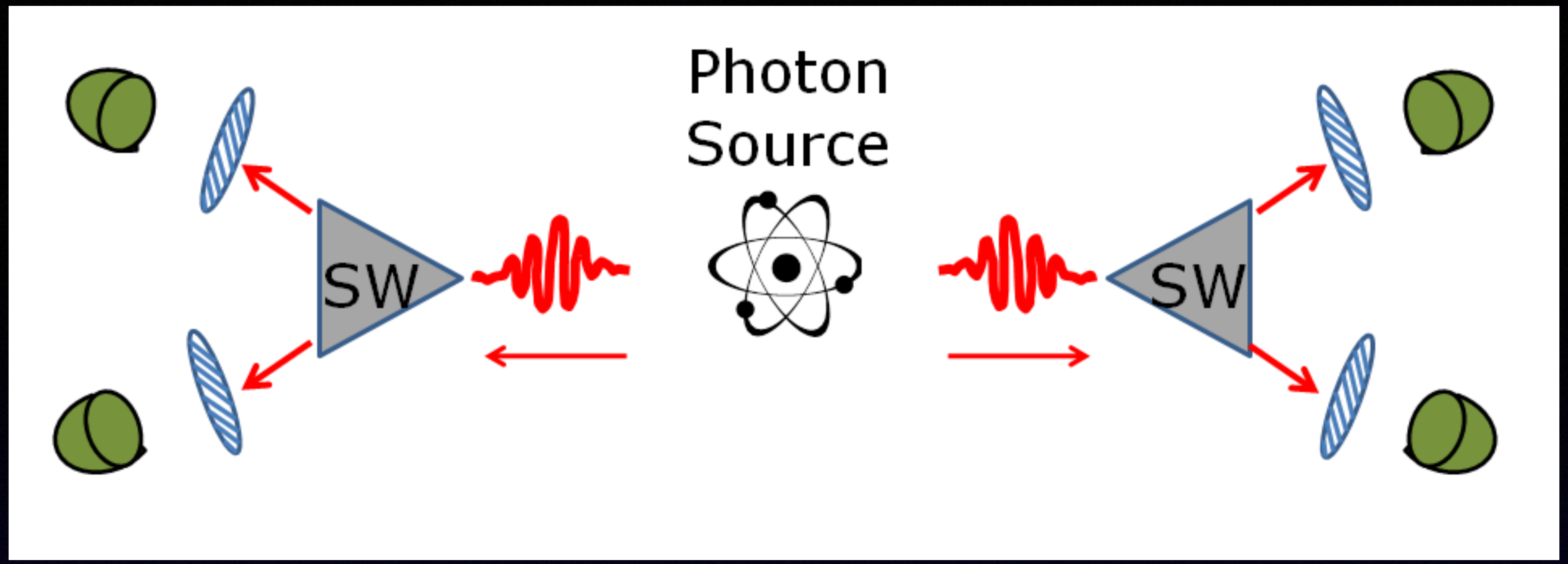
Entanglement can be shared among N particles (→ quantum computers)

Key Aspects of Quantum Entanglement:

- **Non-Separability:** Entangled particles cannot be described individually; they act as a single system.
- **Instant Correlation**: Measuring a property (e.g., spin, polarisation) of one particle instantly determines the state of the other, even if they are light-years apart.
- **Probabilistic Nature:** Before measurement, particles exist in a superposition of states.
- **No FTL Communication:** Although the connection is instantaneous, it cannot be used to transmit information faster than the speed of light.
- **Applications:** It is crucial for quantum computing (qubits), quantum teleportation, and quantum cryptography.

How to produce entangled particles:

Schematic of the third Aspect experiment testing quantum non-locality. Entangled photons from the source are sent to two fast switches, that direct them to polarizing detectors. The switches change settings very rapidly, effectively changing the detector settings for the experiment while the photons are in flight. (Figure by Chad Orzel)



Some Methods to get Quantum Entanglement:

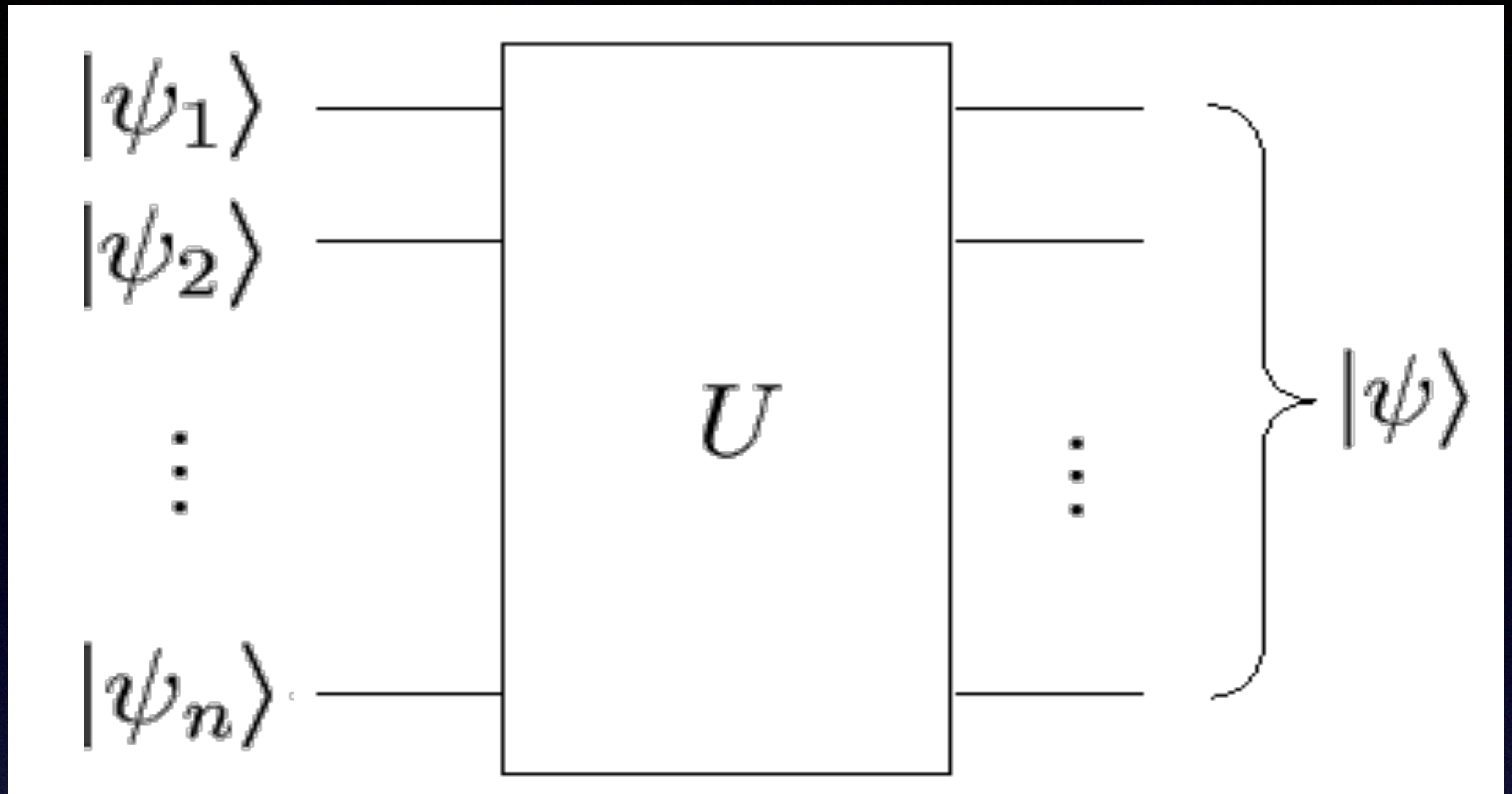
- **Entanglement From Birth**: **emission of two opposite photons/electrons which have opposite polarisations/spins** . Ex: decay of an s=0 particle that produces a $|\text{singlet state}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$
- **Second-Generation Entanglement**: entangled photons are absorbed by identical atoms. Atoms are now entangled.
- **Entanglement by accident:** a pair of atoms at different locations that emit photons. Bringing the photons together in the right way can entangle the states of the two photons, in a way that leads to entanglement of the original atoms.
- **Entanglement by interaction**: Any time you can bring two systems together in such a way that the final state of one particle depends on the input state of the other, you can make an entangled state by making that input state a quantum superposition. This will necessarily lead to a pair of particles each of which is in an indeterminate state, with any eventual measurements of those states being perfectly correlated (or anti-correlated).
- **Spontaneous parametric down-conversion** (also known as **SPDC**, **parametric fluorescence** or **parametric scattering**) is a nonlinear instant optical process that converts one photon of higher energy (namely, a *pump* photon) into a pair of photons (namely, *signal* and *idler* photons) of lower energy, in accordance with the laws of energy conservation and momentum conservation. It is crucial for quantum computing (qubits), quantum teleportation, and quantum cryptography.

Advantages of Qubits & Enormous Quantum Power

- Adding qubits increases storage exponentially
- Quantum computer doubles the power with every added qubit
- To double the power of a digital computer 32bits —> 64 bits
- To double the power of a quantum computer 32 qubits —> 33 qubits
- Can do operations on all superpositions…like massively parallel computation
- One math operation on 2^N numbers encoded in classical computers with N bits requires 2^N steps or parallel processors, but the same operation on 2^N numbers encoded by N qubits requires just 1 step (!!!)
- A 64-bit computer can perform manipulation on 64-bit binary numbers one at at a time.
- A 64-qubit quantum computer operates in a space of 2^{64} dimensions, or roughly16,000,000,000,000,000,000 ($1.6 \cdot 10^{19}$) numbers to specify the state of the quantum system.
- This makes *SOME* complex problems much easier to solve by quantum computer

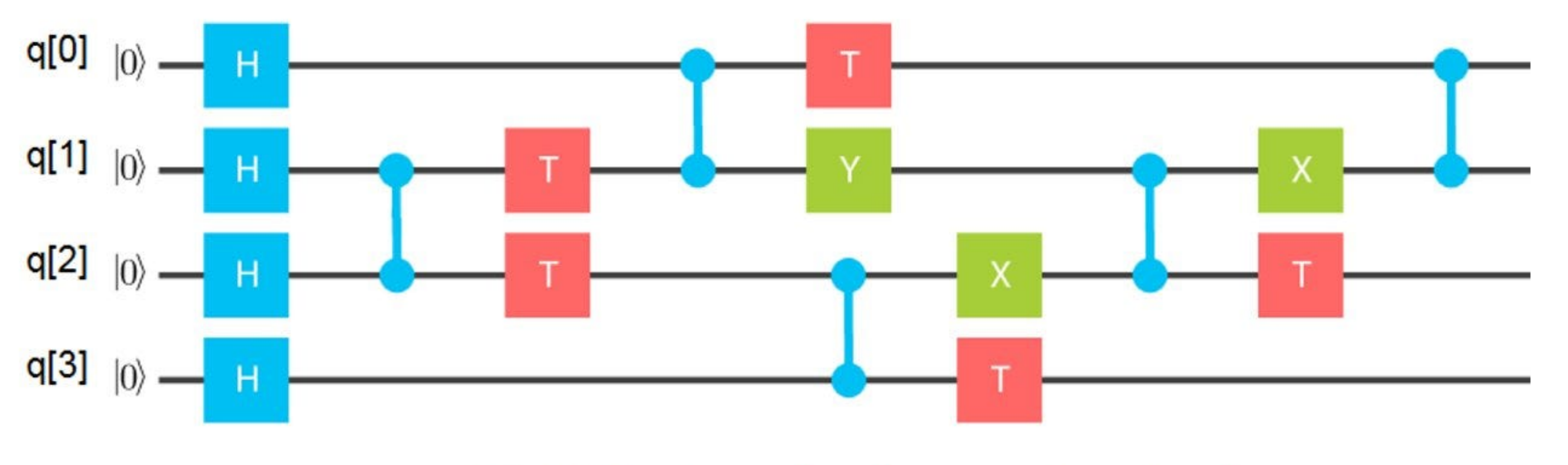
Unitary Transformation as Quantum Computing

On a quantum computer, programs are executed by unitary evolution of an input that is given by the state of the system, $|\psi_n\rangle$, which can in either 0 or 1 state.
Since all unitary operators are invertible, we can always reverse or 'uncompute' a computation on a quantum computer.



Topology of the quantum circuit is fundamental: e.g. entanglement among nearest neighbour only, a few qbits, all qbits.

Schematic of a quantum circuit



(a) A 4x1 universal random quantum circuit

$$\{|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$$

Bell states (entangled) form a 2 qbit basis

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
$$Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y,$$
$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x,$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z.$$

Single qbit gates: X is the NOT operator, Y is the phase shift and Z=XY

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

H is Hadamard gate, S is the phase gate and T is the $\pi/8$ gate

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

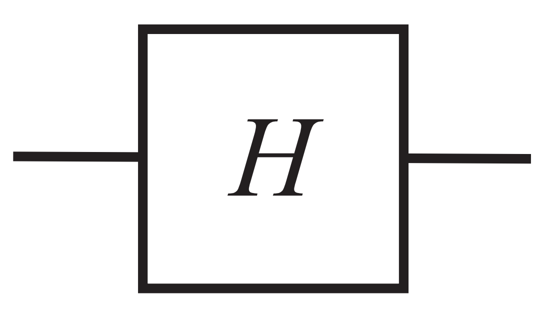
Rotation operators about $\hat{x}$, $\hat{y}$, $\hat{z}$ axis

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$U_{\mathrm{H}} : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

The Hadamard transformation entangles two qbits



Hadamard on N qbits

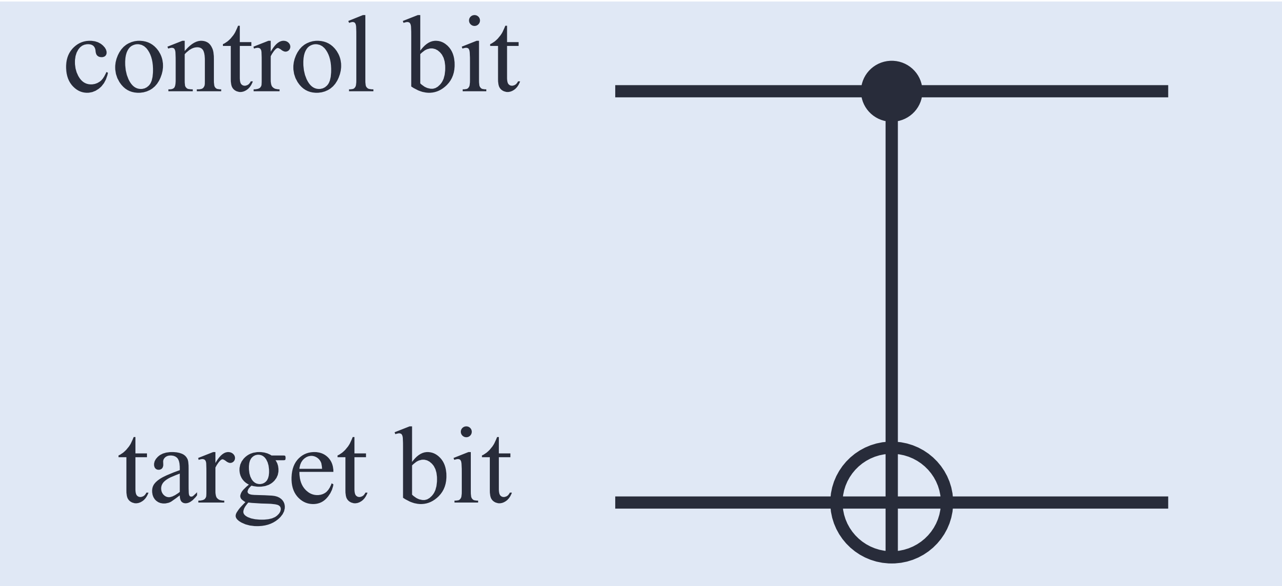
$$(H \otimes H \otimes \ldots \otimes H)|00\ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Two qbit gates: the CNOT (Controlled NOT): the first qbit is the control, the second one is the target. If the first is $|0\rangle$ then the second is unchanged, if the first is $|1\rangle$ then the second is flipped

$$U_{\mathrm{CNOT}} : |00\rangle \mapsto |00\rangle,\ |01\rangle \mapsto |01\rangle,\ |10\rangle \mapsto |11\rangle,\ |11\rangle \mapsto |10\rangle.$$

$$U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$

$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$



Quantum computing hardware comes in various physical implementations:

- Superconducting Quantum Computers: These are the most popular, using superconducting wires and Josephson junctions to create qubits. The two level system is encoded in cooper pairs moving across the junction.
- Quantum Dot and Silicon Spin Quantum Computers: Utilizing fundamental particles like electrons, they encode information in spin or charge of electron to form the two level system whose operations is controlled by microwave/magnetic fields.
- Linear Optical Quantum Computers: These use photons as qubits, manipulating them with optical components like optical mirror or interferometers. A two level system can be a superposition of different path taken by the photon or a superposition of different number of photons present in path.
- Trapped Ion Quantum Computers: Charged atoms are used as qubits, levitating and manipulated with electromagnetic fields. The two level system is the two specific energy levels of an atom.
- Color Center or Nitrogen Vacancy Quantum Computers: Qubits are created from atoms embedded in materials like diamond or silicon carbide. The two level system is the nucleus spin of that embedded atom.
- Neutral Atoms in Optical Lattices: Cold atom physics is used to capture neutral atoms in energy wells, offering another path to quantum simulation. The two level system can be hyperfine energy levels of the atom.
- Topological qbits: uses anyones, 2D quasi-particles, more stable than trapped particles

Strong commercial competition on hardware

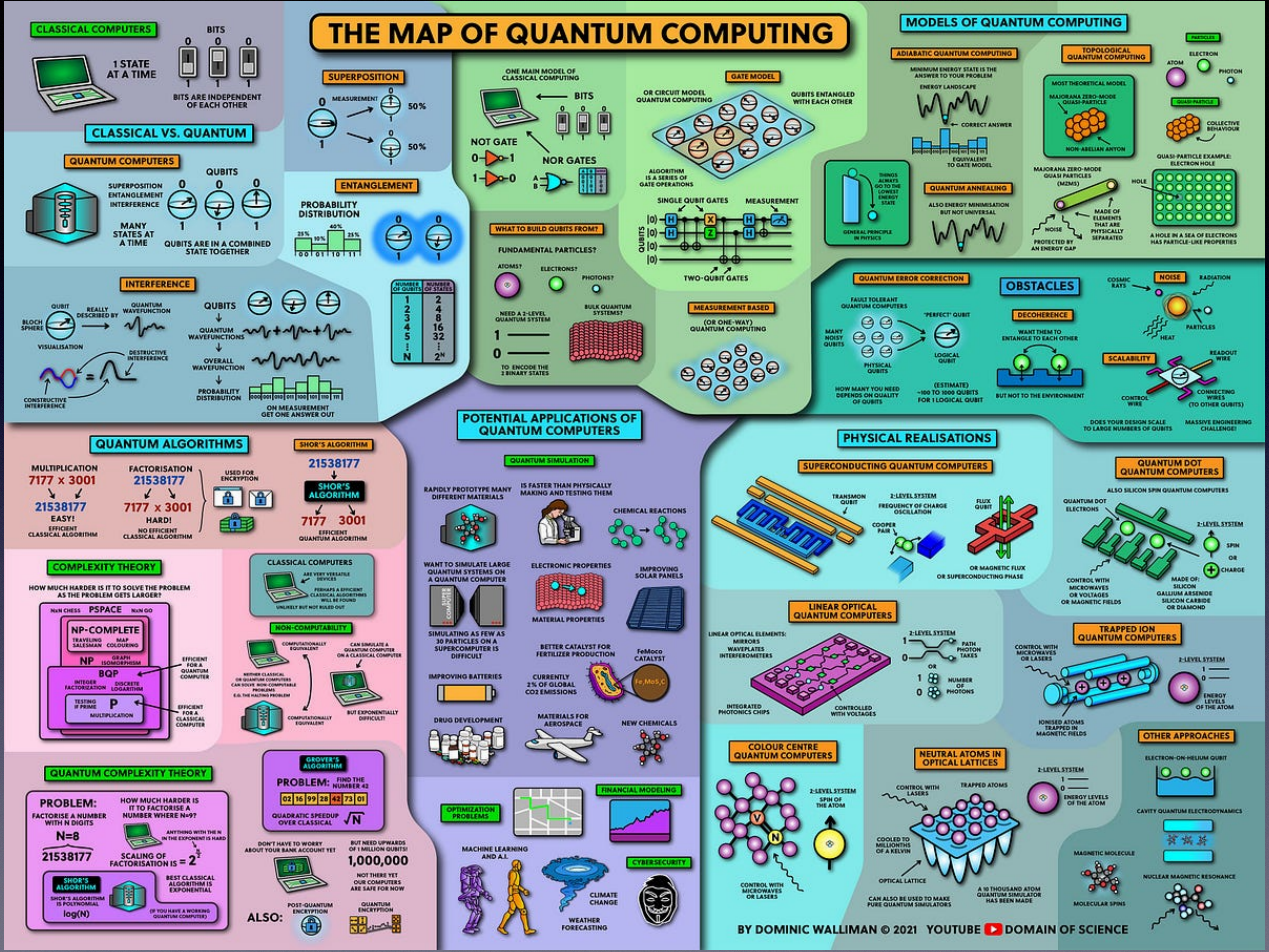
Technology	Used By	Main Advantage	Primary Challenge
Superconducting qubits	IBM, Google, Rigetti	Fast gate speeds, mature tooling	Cryogenic complexity
Trapped ions	IonQ, Quantinuum, Oxford Ionics	High fidelity and coherence	Scaling and control complexity
Topological qubits	Microsoft	Hardware-level error protection	Experimental maturity
Quantum annealing	D-Wave	Commercial optimization today	Limited problem scope
Neutral atoms	Pasqal	Natural scalability	Logical qubit implementation

Promising (?) applications in ASTR*

- multiparameter optimisation, extremal solutions (detection, complex fits/models...)
- Montecarlo & C
- fast search of huge databases [Grover's algorithm]
- Quantum Fourier Transform (SKA?)
- Quantum Machine Learning
- secure space communications (?) [Shor's algorithm]

Problems:

- excessive hype (future backlash?)
- bottleneck in feeding large amount of data
- error mitigation
- others (politics -embargoes- costs, what else)


THE MAP OF QUANTUM COMPUTING
CLASSICAL COMPUTERS
BITS
1 STATE AT A TIME
BITS ARE INDEPENDENT OF EACH OTHER
CLASSICAL VS. QUANTUM
QUANTUM COMPUTERS
QUBITS
SUPERPOSITION
ENTANGLEMENT
INTERFERENCE
MANY STATES AT A TIME
QUBITS ARE IN A COMBINED STATE TOGETHER
SUPERPOSITION
MEASUREMENT
50%
50%
ENTANGLEMENT
PROBABILITY DISTRIBUTION
INTERFERENCE
QUBIT
BLOCH SPHERE
VISUALISATION
QUANTUM WAVEFUNCTION
DESTRUCTIVE INTERFERENCE
CONSTRUCTIVE INTERFERENCE
QUANTUM WAVEFUNCTIONS
OVERALL WAVEFUNCTION
PROBABILITY DISTRIBUTION
ON MEASUREMENT GET ONE ANSWER OUT
NUMBER OF QUBITS
NUMBER OF STATES
ONE MAIN MODEL OF CLASSICAL COMPUTING
NOT GATE
NOR GATES
GATE MODEL
OR CIRCUIT MODEL QUANTUM COMPUTING
QUBITS ENTANGLED WITH EACH OTHER
ALGORITHM IS A SERIES OF GATE OPERATIONS
SINGLE QUBIT GATES
MEASUREMENT
TWO-QUBIT GATES
WHAT TO BUILD QUBITS FROM?
FUNDAMENTAL PARTICLES?
ATOMS?
ELECTRONS?
PHOTONS?
NEED A 2-LEVEL QUANTUM SYSTEM
BULK QUANTUM SYSTEMS?
TO ENCODE THE 2 BINARY STATES
MEASUREMENT BASED
(OR ONE-WAY) QUANTUM COMPUTING
MODELS OF QUANTUM COMPUTING
ADIABATIC QUANTUM COMPUTING
MINIMUM ENERGY STATE IS THE ANSWER TO YOUR PROBLEM
ENERGY LANDSCAPE
CORRECT ANSWER
EQUIVALENT TO GATE MODEL
QUANTUM ANNEALING
ALSO ENERGY MINIMISATION BUT NOT UNIVERSAL
GENERAL PRINCIPLE IN PHYSICS
TOPOLOGICAL QUANTUM COMPUTING
MOST THEORETICAL MODEL
NON-ABELIAN ANYON
MAJORANA ZERO-MODE QUASI PARTICLES (MZMS)
PROTECTED BY AN ENERGY GAP
ELECTRON
ATOM
PHOTON
COLLECTIVE BEHAVIOUR
QUASI-PARTICLE EXAMPLE: ELECTRON HOLE
HOLE
A HOLE IN A SEA OF ELECTRONS HAS PARTICLE-LIKE PROPERTIES
QUANTUM ERROR CORRECTION
FAULT TOLERANT QUANTUM COMPUTERS
"PERFECT" QUBIT
MANY NOISY QUBITS
PHYSICAL QUBITS
LOGICAL QUBIT
HOW MANY YOU NEED DEPENDS ON QUALITY OF QUBITS
(ESTIMATE) ~100 TO 1000 QUBITS FOR 1 LOGICAL QUBIT
OBSTACLES
DECOHERENCE
WANT THEM TO ENTANGLE TO EACH OTHER
BUT NOT TO THE ENVIRONMENT
NOISE
COSMIC RAYS
RADIATION
HEAT
PARTICLES
SCALABILITY
READOUT WIRE
CONTROL WIRE
CONNECTING WIRES (TO OTHER QUBITS)
DOES YOUR DESIGN SCALE TO LARGE NUMBERS OF QUBITS
MASSIVE ENGINEERING CHALLENGE!
QUANTUM ALGORITHMS
MULTIPLICATION
7177 x 3001
21538177
EASY!
EFFICIENT CLASSICAL ALGORITHM
FACTORISATION
21538177
7177 x 3001
HARD!
NO EFFICIENT CLASSICAL ALGORITHM
USED FOR ENCRYPTION
SHOR'S ALGORITHM
21538177
SHOR'S ALGORITHM
7177 3001
EFFICIENT QUANTUM ALGORITHM
COMPLEXITY THEORY
HOW MUCH HARDER IS IT TO SOLVE THE PROBLEM AS THE PROBLEM GETS LARGER?
PSPACE
NP-COMPLETE
TRAVELING SALESMAN
MAP COLOURING
NP
GRAPH ISOMORPHISM
BQP
INTEGER FACTORIZATION
DISCRETE LOGARITHM
P
TESTING IF PRIME
MULTIPLICATION
EFFICIENT FOR A QUANTUM COMPUTER
EFFICIENT FOR A CLASSICAL COMPUTER
CLASSICAL COMPUTERS
ARE VERY VERSATILE DEVICES
NON-COMPUTABILITY
COMPUTATIONALLY EQUIVALENT
CAN SIMULATE A QUANTUM COMPUTER ON A CLASSICAL COMPUTER
BUT EXPONENTIALLY DIFFICULT!
QUANTUM COMPLEXITY THEORY
PROBLEM:
FACTORISE A NUMBER WITH N DIGITS
N=8
21538177
HOW MUCH HARDER IS IT TO FACTORISE A NUMBER WHERE N=9?
SCALING OF FACTORISATION IS = 2
BEST CLASSICAL ALGORITHM IS EXPONENTIAL
SHOR'S ALGORITHM
SHOR'S ALGORITHM IS POLYNOMIAL
log(N)
GROVER'S ALGORITHM
PROBLEM: FIND THE NUMBER 42
02 16 99 28 42 73 01
QUADRATIC SPEEDUP OVER CLASSICAL
√N
DON'T HAVE TO WORRY ABOUT YOUR BANK ACCOUNT YET
BUT NEED UPWARDS OF 1 MILLION QUBITS!
1,000,000
NOT THERE YET OUR COMPUTERS ARE SAFE FOR NOW
ALSO:
POST-QUANTUM ENCRYPTION
QUANTUM ENCRYPTION
POTENTIAL APPLICATIONS OF QUANTUM COMPUTERS
QUANTUM SIMULATION
RAPIDLY PROTOTYPE MANY DIFFERENT MATERIALS
IS FASTER THAN PHYSICALLY MAKING AND TESTING THEM
CHEMICAL REACTIONS
WANT TO SIMULATE LARGE QUANTUM SYSTEMS ON A QUANTUM COMPUTER
ELECTRONIC PROPERTIES
IMPROVING SOLAR PANELS
MATERIAL PROPERTIES
SIMULATING AS FEW AS 30 PARTICLES ON A SUPERCOMPUTER IS DIFFICULT
BETTER CATALYST FOR FERTILIZER PRODUCTION
FeMoco CATALYST
IMPROVING BATTERIES
CURRENTLY 2% OF GLOBAL CO2 EMISSIONS
DRUG DEVELOPMENT
MATERIALS FOR AEROSPACE
NEW CHEMICALS
OPTIMIZATION PROBLEMS
FINANCIAL MODELING
MACHINE LEARNING AND A.I.
CYBERSECURITY
CLIMATE CHANGE
WEATHER FORECASTING
PHYSICAL REALISATIONS
SUPERCONDUCTING QUANTUM COMPUTERS
TRANSMON QUBIT
2-LEVEL SYSTEM
FREQUENCY OF CHARGE OSCILLATION
COOPER PAIR
FLUX QUBIT
OR MAGNETIC FLUX OR SUPERCONDUCTING PHASE
QUANTUM DOT QUANTUM COMPUTERS
ALSO SILICON SPIN QUANTUM COMPUTERS
QUANTUM DOT ELECTRONS
2-LEVEL SYSTEM
SPIN
OR
CHARGE
CONTROL WITH MICROWAVES OR VOLTAGES OR MAGNETIC FIELDS
MADE OF: SILICON GALLIUM ARSENIDE SILICON CARBIDE OR DIAMOND
LINEAR OPTICAL QUANTUM COMPUTERS
LINEAR OPTICAL ELEMENTS: MIRRORS WAVEPLATES INTERFEROMETERS
2-LEVEL SYSTEM
PATH PHOTON TAKES
NUMBER OF PHOTONS
INTEGRATED PHOTONICS CHIPS
CONTROLLED WITH VOLTAGES
TRAPPED ION QUANTUM COMPUTERS
CONTROL WITH MICROWAVES OR LASERS
2-LEVEL SYSTEM
ENERGY LEVELS OF THE ATOM
IONISED ATOMS TRAPPED IN MAGNETIC FIELDS
COLOUR CENTRE QUANTUM COMPUTERS
2-LEVEL SYSTEM SPIN OF THE ATOM
CONTROL WITH MICROWAVES OR LASERS
NEUTRAL ATOMS IN OPTICAL LATTICES
CONTROL WITH LASERS
TRAPPED ATOMS
2-LEVEL SYSTEM
ENERGY LEVELS OF THE ATOM
COOLED TO MILLIONTHS OF A KELVIN
OPTICAL LATTICE
CAN ALSO BE USED TO MAKE PURE QUANTUM SIMULATORS
A 10 THOUSAND ATOM QUANTUM SIMULATOR HAS BEEN MADE
OTHER APPROACHES
ELECTRON-ON-HELIUM QUBIT
CAVITY QUANTUM ELECTRODYNAMICS
MAGNETIC MOLECULE
MOLECULAR SPINS
NUCLEAR MAGNETIC RESONANCE
BY DOMINIC WALLIMAN © 2021 YOUTUBE DOMAIN OF SCIENCE