Introduction to Quantum Computing

Federico Matteoni

A.A. 2021/22

Index

0.1 Introduction

Prof.: Anna Bernasconi, Gianna del Corso

What is Quantum Computing? Quantum computing concerns the **relationship between physics and computer science**. Physical phenomenon apply to information and computation: a **computational process is seen as a physical process**, performed on a machine whose operation obey certain physical laws.
The classical theory of computation is based on the Universal Turing Machine, a mathematical abstraction and **not a physical device**, that works according to a set of rules and principles enunciated in 1936 and elaborated in the 1940s.

Church-Turing Thesis *Every function which would naturally be regarded as computable can be computed by the Universal Turing Machine.*
A stronger version: every function that we can compute efficiently on any machine efficiently on a Universal Turing Machine. So we can solve a problem if and only if we can solve it on a Turing machine.

The assumption underlying these principles is that a Turing machine idealizes a mechanical computing device that obeys the laws of classical physics, but nature is better described by the laws of quantum physics. Feynman stated that "*nature isn't classical*", and that our model of computations (i.e. classical computers) cannot efficiently model quantum systems in a scalable manner. They seem to be extraordinarily slow and inefficient at doing quantum simulations.

David Deutsch "*Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not pure mathematics.*"
Is there a single universal computing device which can efficiently simulate any other physical system? To answer this, Deutsch proposed a new type of computing system: quantum computers.
Quantum computers can do everything that conventional computers can do, but are also capable of efficiently simulate quantum-mechanical processes. And so they are **more natural computing models than conventional computers**.

What is quantum? Quantum physics is a mathematical model first used to describe physical phenomena that occur at the microscopic level, such as inside an atom, which exposed gaps in the preceding theory of classical physics. Quantum theory explains this behavior and gives us a more complete picture of the universe. The description of the universe given by quantum physics differs in fundamental ways from the classical description, and is often at odds with our intuition which has evolved according to observation of macroscopic phenomena (which are, to an extremely good approximation, classical physics).

An experiment Let us consider an experiment that could not be explained in a natural way using classical physics. This experiment involves photons:

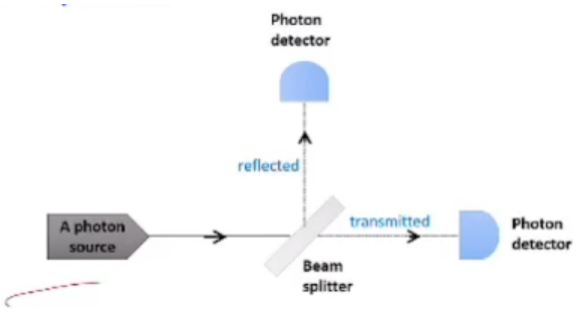
elementary particles (**quantum**) of light

massless

move at the speed of light in vacuum ($\simeq 3 \cdot 10^8$ m/s)

exhibit wave-particle duality: behavior featuring properties of both waves and particles

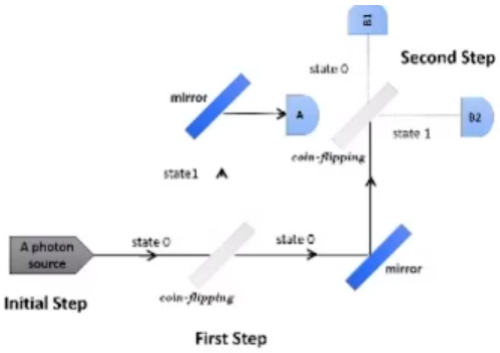
We need a photon source, a beam splitter (implemented using a half silvered mirror) and a pair of photon detectors. We will trace the behavior of the photons.



We send a series of individual photons along a path from the source towards the splitter. We expect two behaviors: the beam splitter transmits or reflects the photon. We observe the photon arriving at the detector on the right of the splitter half of the time, and arriving at the detector above half of the time.
So, we can model the splitter as flipping a fair coin, and choosing whether to transmit or reflect the photon based on the result of the coin-flip.

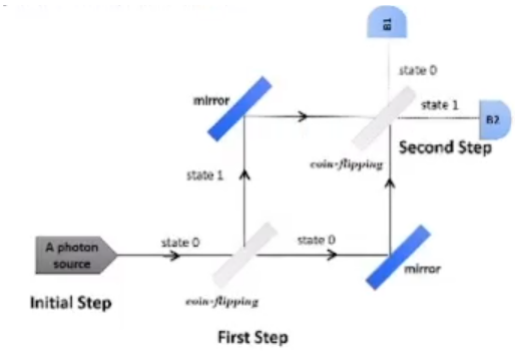
A beam splitter behaves like a fair coin: head (state 0) → transmitted, tail (state 1) → reflected. So both detectors will expect a photon with probability $\frac{1}{2}$

Second experiment We extend the experiment with two mirrors and another beam splitter.



We have three detectors, and we observe a photon in A with probability $\frac{1}{2}$, and in B1 or B2 with probability both $\frac{1}{4}$. Both experiments confirms our prediction.

Third experiment Let's remove the detector A.



So we flip our photon, the "quantum coin", **without looking at the result of the first splitter**. What are the probabilities of observing the photon in B1 or B2? With the classical intuition, we expect $\frac{1}{2}$ probability in both and that's what would happen with a real "macroscopic" coin. So we predict to observe the photon in B1 and B2 evenly. Let's see it in a mathematical way:

State 0: transmitted

State 1: reflected

With a vector representation:

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

With $|\ \rangle$ called **Dirac notation**, standard notation for states in quantum mechanics.
Uncertain states will be represented by linear combinations of $|0\rangle$ and $|1\rangle$

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

With α_0, α_1 being the probabilities of finding the photon in state $|0\rangle$ or $|1\rangle$.
Since we should find the photon in exactly one path, we must have $\alpha_0 + \alpha_1 = 1$

We model the splitter as randomly selecting whether the photon will be transmitted (state $|0\rangle$) or reflected (state $|1\rangle$)
After the initial step, we are in $|0\rangle$. We flip a coin (first splitter): the new probabilistic state is expected to be in both states with probability $\frac{1}{2}$

$$\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

The transition of a far coin can be represented by the matrix

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

When the photon passes through the splitter, we multiply its state vector by this matrix, to derive the new state where the photon is expected to be in both states $|0\rangle$ and $|1\rangle$ with probability $\frac{1}{2}$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Then we flip the coin again, and multiply the new state vector by the same matrix. The new probabilistic state will be the same:

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

So our mathematical model confirms our expectations.

The experimental results do not agree with our classical intuition! We observe the photons **only in B1** and we **never observe any photon in B2**. This is the same problem which led to the development of quantum physics.

Quantum Physics So let's use quantum physics to explain our experiments. "*Quantum theory is probability theory with negative numbers*", but we can't have negative probabilities so we will use a new quantity called **amplitude**. To get around the fact that we cannot have negative probabilities and that all our probabilities must add up to 1, we use a mathematical trick: we square our amplitudes to calculate the probabilities.
According to the quantum mechanical description, the beam splitter causes the photon to go into a **superposition** of both states. Mathematically, we describe such superposition by taking a linear combination of the state vectors with α_0 and α_1 now being **complex numbers** $\in C$. If we measure the photon to see its state, we find it in state $|0\rangle$ with probability $|\alpha_0|^2$ and in state $|1\rangle$ with probability $|\alpha_1|^2$, and since a photon should be find in exactly one path, we need $|\alpha_0|^2 + |\alpha_1|^2 = 1$

We start in state $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. When it passes through the first splitter, we multiply its state vector with the matrix

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

After passing through the first splitter:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Same as before, with $\frac{1}{\sqrt{2}}$ instead of $\frac{1}{2}$. The result correspond with the observed behavior: we measure the photon in state $|0\rangle$ with probability $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ and in state $|1\rangle$ with probability $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. The photon is in a **superposition** of states $|0\rangle$ and state $|1\rangle$, being in both states with amplitudes $\frac{1}{\sqrt{2}}$ and $\frac{1}{\sqrt{2}}$ respectively.
If we do not measure the state of the photon after passing through the first beam splitter, then its state remains $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. If the photon is allowed to pass through the second splitter before any measurement, the new state vector becomes

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} + \frac{1}{2} \\ \frac{1}{2} - \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The amplitude of the state $|0\rangle$ becomes 1, but the amplitude of the state $|1\rangle$ becomes 0 because **the amplitudes of finding the photon in state** $|1\rangle$ **cancel each other out**. We call this effect **interference**.
After being in both states at the same time with certain amplitudes, by passing through a second splitter the outcomes are interfered with each other: the interference can be destructive ($\frac{1}{2} - \frac{1}{2}$) or constructive ($\frac{1}{2} + \frac{1}{2}$).

What is Quantum Computing? If we measure the photon, we find it coming out of state $|0\rangle$ with probability 1. Thus, after the second splitter the photon is entirely in state $|0\rangle$, which is what we observed.
In quantum "language": the second splitter has caused the two states (in superposition) to interfere, resulting in the cancellation of state $|1\rangle$.
The interference effects can be used to our advantage. We can combine operations such as the quantum coin toss to build more efficient algorithms. These algorithms can use interference effects to make the wrong answers cancel out quickly and give us high probabilities of measuring the right answer. This is the idea behind quantum computing.

Observations

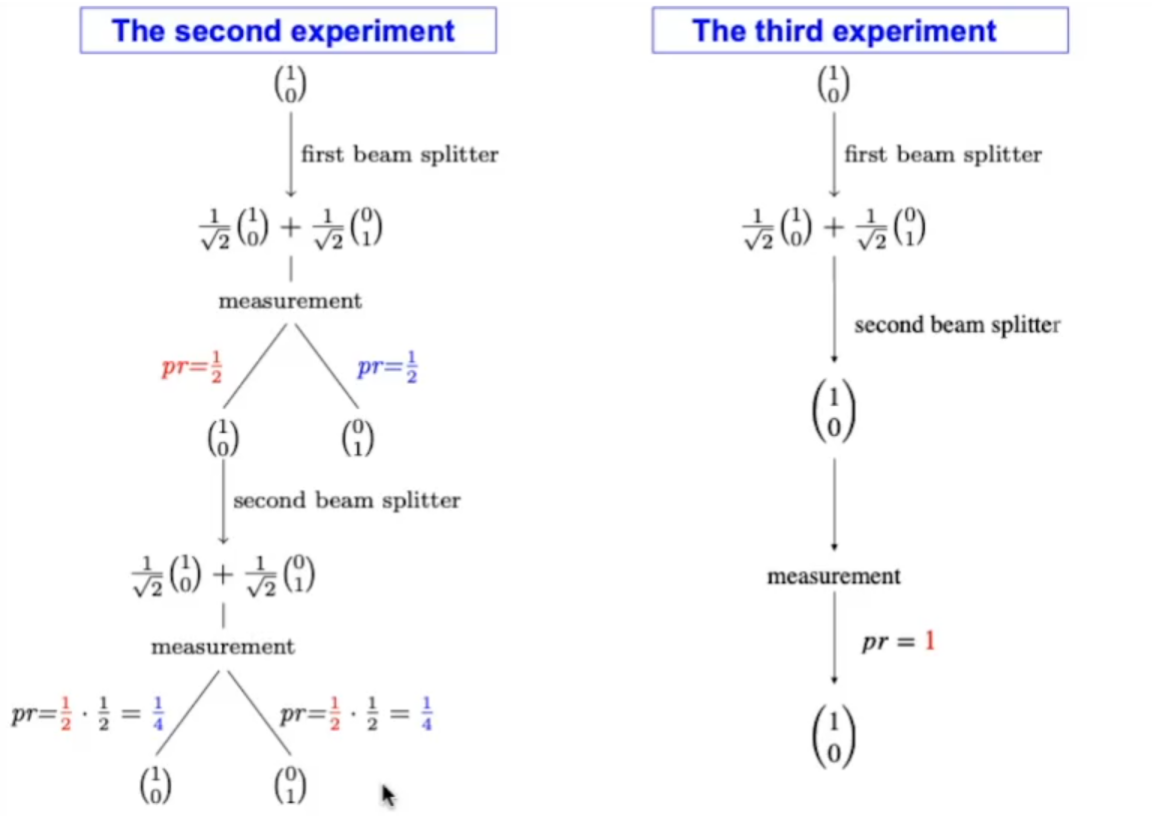
This model works when the initial state is $|1\rangle$

This model works also with complex numbers
For instance we could use:

Transition matrix: $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$

Superposition of state $|0\rangle$ and $|1\rangle$: $\frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}$

The model is consistent with the first and second experiment



Phenomena of quantum mechanics that may intervene in the processing of information

Superposition Property of a quantum system to be in different states at the same time.
A quantum system can be in more than one state at the same time with non-zero amplitudes: we say that it's in a superposition of these states. When evolving from a superposition, the resulting transitions may affect each other constructively and destructively. This happens because of having opposite sign transition amplitudes

Decoherence The attempt to observe or measure the state of the system causes its collapse towards a single state.
The probability of a system to be observed in a specific state is the square value of its amplitude of a state. After the measurement, the system is no longer in a superposition: the information kept in the superposition is lost.
The experimental manipulation of quantum systems is extremely difficult because every minimal disturbance

can determine the decoherence.
Qubits interact with their environments to some degree, even thought the physical substrate used to store them has been designed to keep the isolated.

No-Cloning It's impossible to create an independent and identical copy of an arbitrary unknown quantum state

Entanglement Possibility that two or more elements are in quantum states completely correlated with each other so that, even if transported at a great distance from each other, they maintain the correlation.

0.1.1 Quantum Computer

Bit and qubit Conventional computers are made up of bits, while quantum computers are made up of quantum bits, or **qubits**.
A bit is the fundamental concept of classical computation: we can think of it in abstract terms as having a state which is either 0 or 1.
A qubit is the simplest of all quantum systems:

like a bit, it has a state

two special states for qubits are the state $|0\rangle$ and $|1\rangle$, which correspond to states 0 and 1 of classical bits

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

These are called **computational basis states** and form an orthonormal basis for C^2

The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ and $|1\rangle$: it can be in a superposition of the two states simultaneously

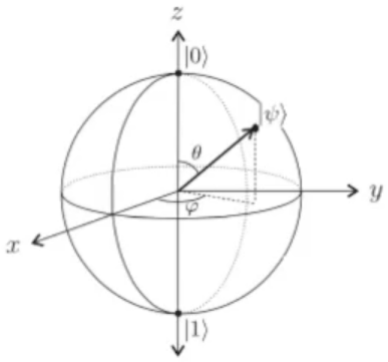
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The representation of information is binary, but each qubits contains double information with respect to a bit.

We can examine a bit to determine if it's in state 0 or 1, but we cannot examine a qubit to determine it's quantum state (the values of α and β). We can only acquire much more restricted information about the quantum state.

Measuring a qubit can only give classical results: either 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$
Note that by measuring we lose information.

A qubit $|\psi\rangle$ can be represented in a three-dimensional space as a point on the surface of a sphere of unitary radius known as **Bloch's sphere**.



How much information in a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$? α is a complex number and we could store lots of bits in the binary expression of $\mathrm{Re}(\alpha)$. This is there was some way of measuring the value of α exactly. But α, β are kind of hidden information. Measurement of a qubit will give only a single bit of information, 0 or 1, about the state of the qubit. There is no way to figure out α and β if they start out unknown: after the measurement α and β are gone.
Why does this collapse occurs? We don't know.
Only if infinitely many identically prepared qubits

Power of Quantum Computing The system can be put in a combination of very large number of state: n qubits in a superposition of 2^n states, so operating on 2^n bits at the same time.
Idea: find an algorithm that converges all 2^n states of the qubits to a state that's solution of the problem: exploiting constructive and destructive interferences, for example.

Quantum Algorithms We start from a well known initial state (example: all qubits in $|0\rangle$). The system evolves in a quantum way: qubits are connected in elementary logic circuits and are manipulated by a simple set of rules (rotations of state vectors of the quantum state).
From a superposition of states to a superpositions of calculations (each with a certain probability of converging to a significant result) to a superposition of results. When the machine measures the final state, the superposition of results collapses on the result with the higher probability: with high probability being the solution of our problem.
This can be called **quantum parallelism**.

> Observing the system during these manipulations comes with a severe **penalty**: if we look to soon, the **computation will fail**. We are allowed to **view only the machine final state**.
>
> Interaction with the outside occurs through classic bit sequences: qubits collapses in that instant to a single state.

Why Quantum Computing? The idea was born to efficiently simulate quantum-mechanical processes. But this model can help to solve problems of high computational complexity.
However:

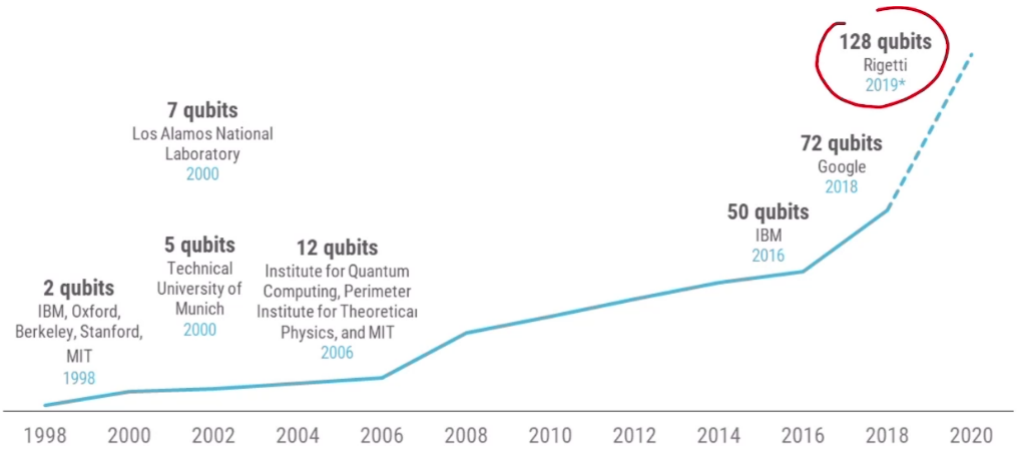
> Quantum computation doesn't violate the Church-Turing thesis, undecidable functions are still undecidable
>
> Widely believed that NP-Complete problems are still difficult problems, requiring exponential time

We are interested because for some problems a classical computers can take exponentially more time.

Shor's Factoring Algorithm Factor numbers in polynomial time. This remains one of the (or *the*) most important results in quantum computing. Meaning that **current public key cryptography can be attacked**. But remember that factorization is not NP-complete.

Grover's Quantum Search The algorithm concerns search in an unstructured database with N entries. If we are searching for a unique marked entry, classicaly it would take a maximum of N queries and $\frac{N}{2}$ queries on average.
With this algorithm, enables the search to be completed with $O(\sqrt{N})$ queries. It's **optimal**: no search algorithm can do less than $\sqrt{N}$ operations.
In practice, this quadratic speed-up can be very impactful making a big difference. With 10^{20} entries, and a quantum processors capable of 10^8 calls per second, we can find the entry in 10^{10} calls, so 10^2 seconds ($\simeq$ 2 minutes). In classical search we would need 10^{12} seconds ($\simeq$ 32000 years).
In cryptography, it enables brute force attacks so we need longer keys.

Evolution of Quantum Technology



IBM claims that it will build a 1000-qubit machine by 2023 and 1M-qubits by 2030.

Quantum Supremacy Is the goal of demonstrating that a programmable quantum device can solve a problem that **no classical computer can solve in any feasible amount of time** (irrespective of the usefulness of the problem). Proving this requires:

Building a powerful physical quantum machine

Finding a problem that can be solved efficiently on a quantum computer with a superpolynomial speed-up over the best known or possible classical algorithm for that task.

Note that Shor's algorithm is unfeasible to be implemented with current technology, so it cannot be used to prove quantum supremacy.

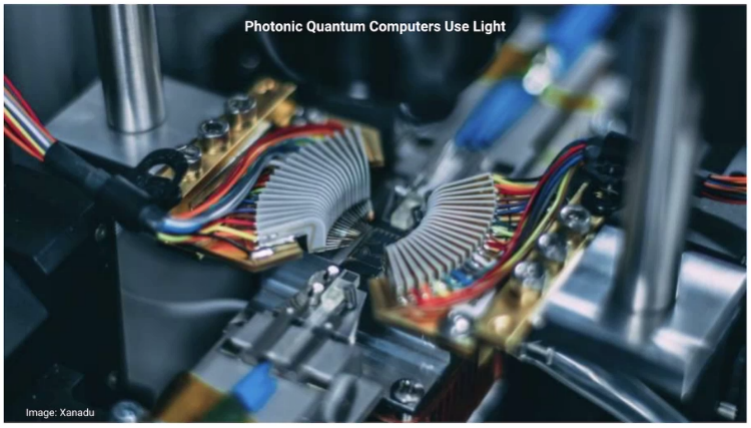
Physical Realization of Quantum Computers A qubit can be realized as real quantum physical system. We can use:

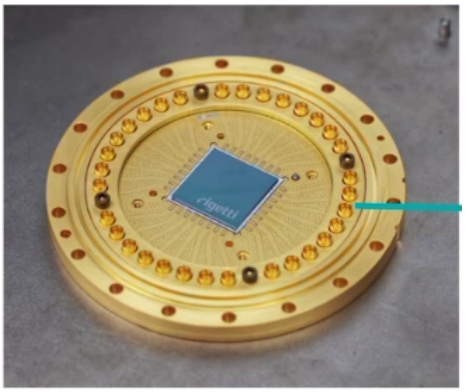
Two different polarization of a photon

Two possible alignments of nuclear spin in a uniform magnetic field

Two state of an electron orbiting a single atom (ground or excited state, shining light on the electron makes it change states and even stay halfway between states)

The theory is independent of the physical realization of the system.

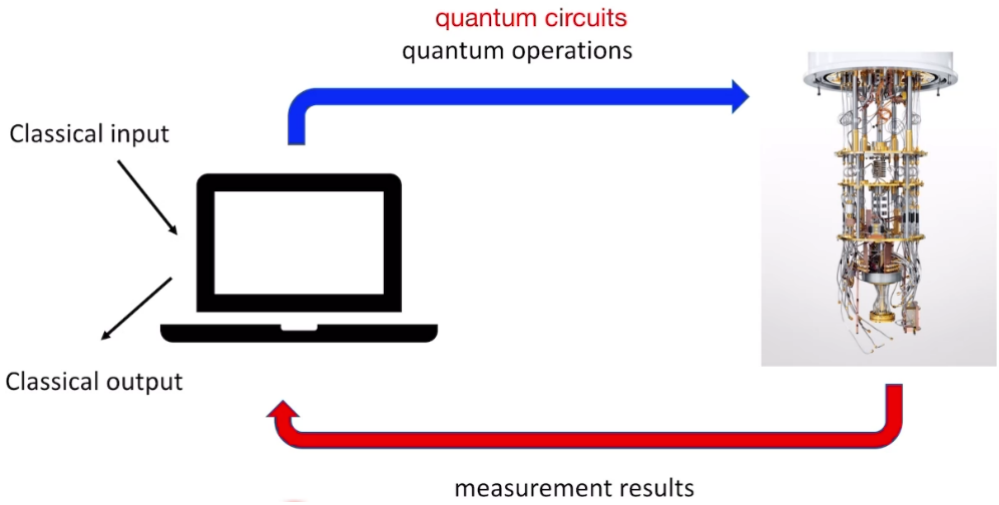




Quantum processor

Challenges It will be quite an engineering challenge to control a quantum computer and to make sure that its state will not be affected by various sources of error.
Quantum operations (rotations) are never perfect: an intended rotation of 90 degrees might end up being of 90.1 or 89.9 degrees and this errors add up quickly.
It's very difficult to avoid interaction with the external environments, so need fault-tollerant protocols and quantum-errors correcting algorithms, meaning additional qubits.
Circuit dimensions are also very large. Shor's algorithm require $O(n^2 \log n \log\log n)$ gates for a n bit number.

0.2 Circuit Model of Computation



The **interaction is classical**.

Circuits Networks (graphs) of wires (arcs) that carry bit values to gates that perform elementary operations (nodes) on the bits (input nodes).
C_n circuit with n input variables. We consider acyclic circuits. The gates come from some finite library of gates.
Circuits are a **non-uniform model of computation**: with n inputs we can solve only instances of length n. Inputs of different lengths are processed by different circuits, in contrast with uniform models (such as Turing machines) where the same computational device is used for all possible input lengths. A different "program" for each input size.

Non-uniform because computation on input size n can be absolutely different from computations on some input size m. For example, **non-uniform circuit families of small size may compute undecidable functions**. Size being the number of operations in the circuit.

> Let $L \subseteq \{0,1\}^*$ be an undecidable language
>
> Let $U = \{1^n \mid \text{the binary expansion of } n \text{ is in } L\}$
> For example $1^5 = 11111_1 \in U$ if $5_{10} = 101_2 \in L$
>
> U is also undecidable, but we can build a non-uniform family of circuits that computes U: $\forall\, n$ we build two circuits with n inputs
>
> C_n^0
> C_n^1
>
> What's missing is the effective and efficient constructability of the circuits. Since U is undecidable we are not able to say if the n-th circuit of the family is C_n^0 or C_n^1.

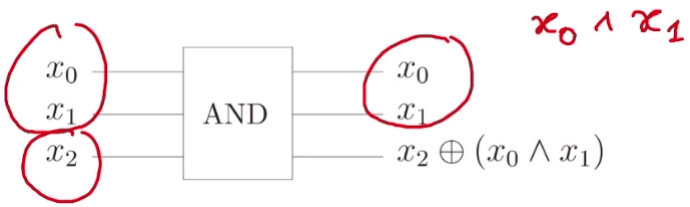
Uniform Families So we often impose a **uniformity condition**: the family is uniform if each C_n can be constructed by an appropriately resource-bounded Turing machine. We assume that the circuits can be generated by a Turing machine or equivalent model that on input n produces a description of C_n in time polynomial in n and in the number of gates in C_n.

Complexity of the Circuits One natural measure is the **overall number of gates**, the number of operations (can be put in relation with sequential time).
Another is the **depth of the circuit**, the length of the longest path between input and output with each gate counting as one, can be put in relation with parallel time.
A third measure is the **number of input variables**, sometimes called width or space of the circuit.

Reversible Computation Quantum computation are always reversible. A computation is reversible if it always possible to uniquely recover the input given the output. Otherwise, it's called irreversible.
Many classical logic gates are irreversible, but the NOT gate is reversible.
Reversibility is connected to information loss: an irreversible operation produces loss of information. With reversible computation no information is ever erased.
Laws of physics

Reversible Circuits Realize bijection. We have digital circuits with same number of input and outputs. Any classical irreversible circuit can be transformed in a equivalent reversible one (computes same one), by adding new inputs and new outputs and replacing irreversible operations with reversible ones. The extra inputs represent information that we must keep in order to maintain the reversability.
With an irreversible classical circuit of depth T and space S, the reversible version uses $O(S+ST)$ space and T depth.

Reversible AND Also known as Toffoli gate.



Universality A set of gates is universal for classical computation if, for any positive integer n, m and any function $f : \{0,1\}^n \to \{0,1\}^m$, a circuit can be constructed for computing f using only gates from that set.
Well-known sets are {AND, OR, NOT}...
NAND and NOR gates have the **functional completeness** assuming unlimited unlimited fanout (a gate can be connected to unlimitedely many nodes).

Toffoli gate is universal for classical reversible computation. We need to add **ancillary** (extra) bits that can be initialized to 0 or 1 as required.