# 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:

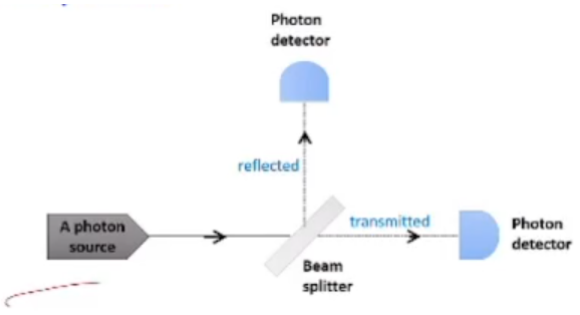
elementary particles (**quantum**) of light

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

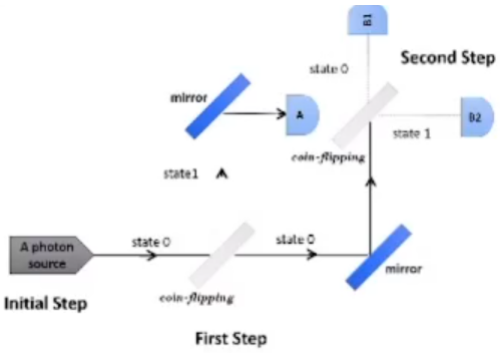
We need a photon source, a beam splitter (implemented using a half silvered mirror) and a pair of photon detectors. We will trace the behavior of the photons.



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.

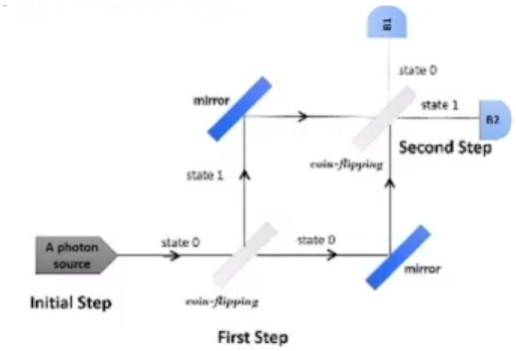
A beam splitter behaves like a fair coin: head (state 0) → transmitted, tail (state 1) → reflected. So both detectors will expect a photon with probability $\frac{1}{2}$

**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 $\alpha_0, \alpha_1$ 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 $\alpha_0$ and $\alpha_1$ 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**

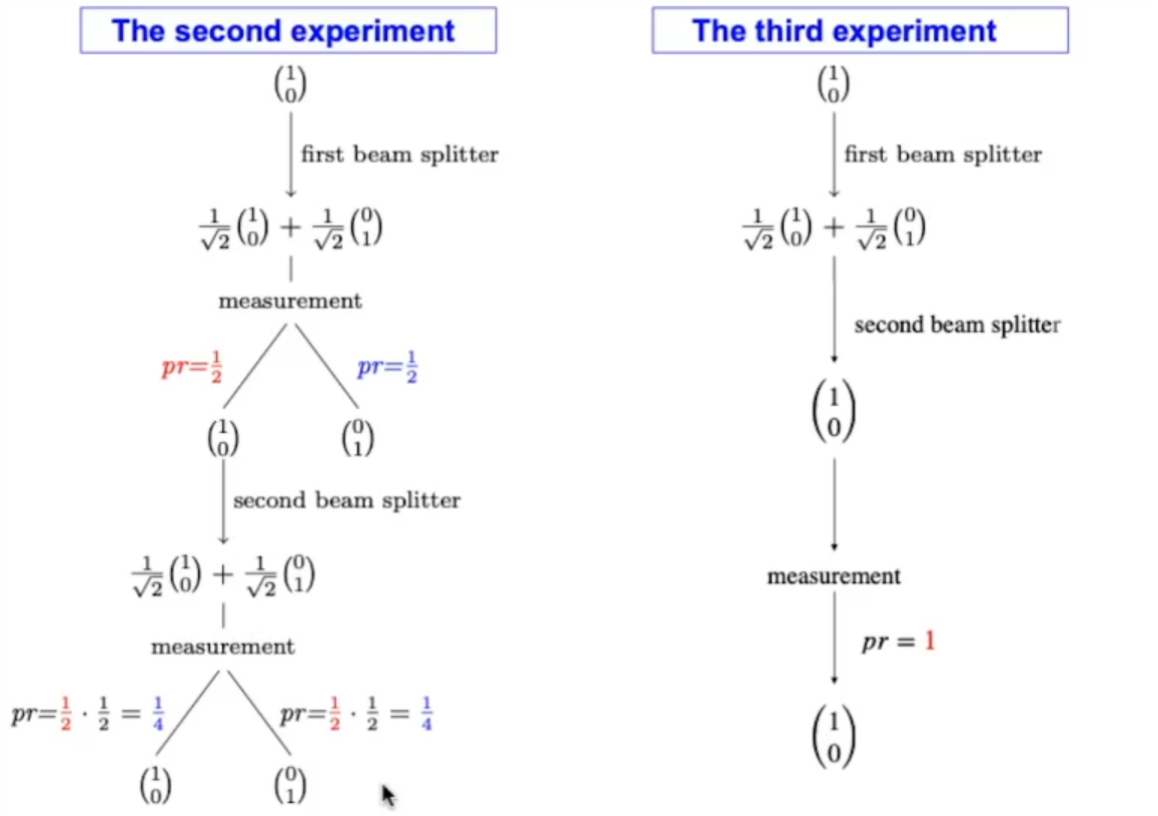
This model works when the initial state is $|1\rangle$

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

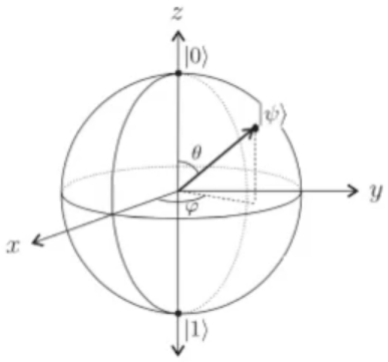
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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 $\alpha$ and $\beta$). 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 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$? $\alpha$ 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 $\alpha$ exactly. But $\alpha, \beta$ 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 $\alpha$ and $\beta$ if they start out unknown: after the measurement $\alpha$ and $\beta$ 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:

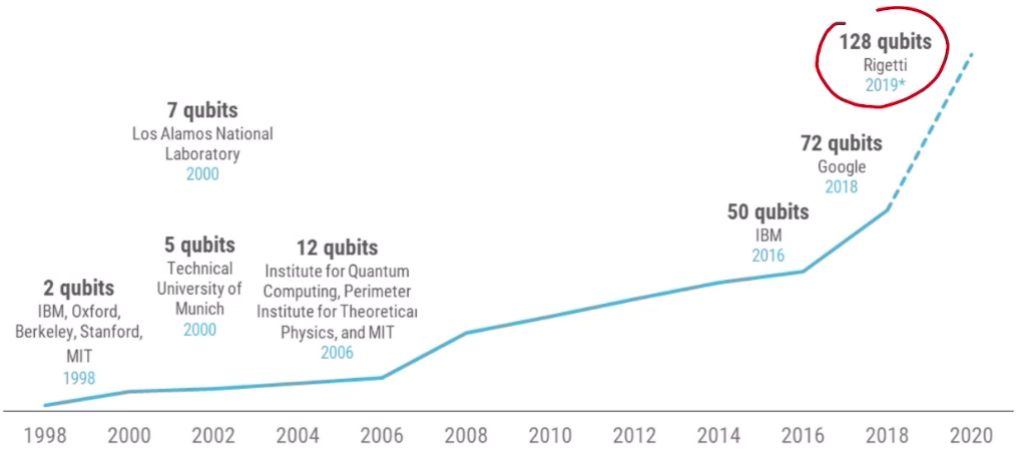
> Quantum computation doesn't violate the Church-Turing thesis, undecidable functions are still undecidable
>
> Widely believed that NP-Complete problems are still difficult problems, requiring exponential time

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.

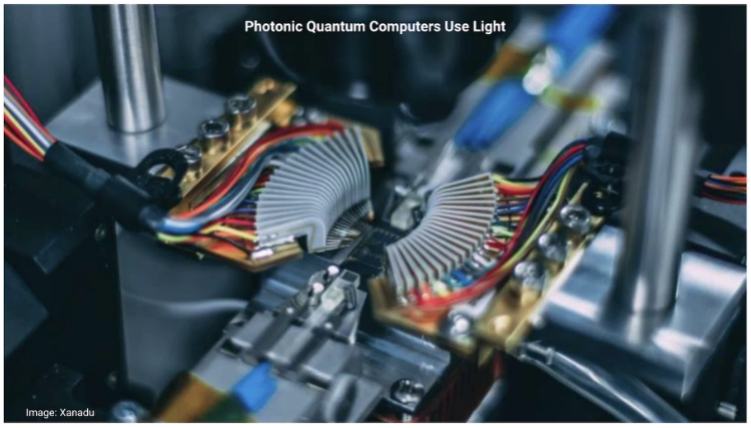
**Physical Realization of Quantum Computers** A qubit can be realized as real quantum physical system. We can use:

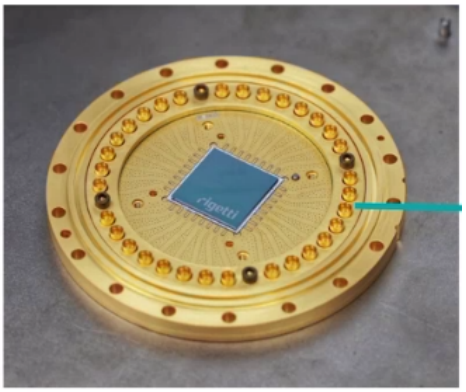
Two different polarization of a photon

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.

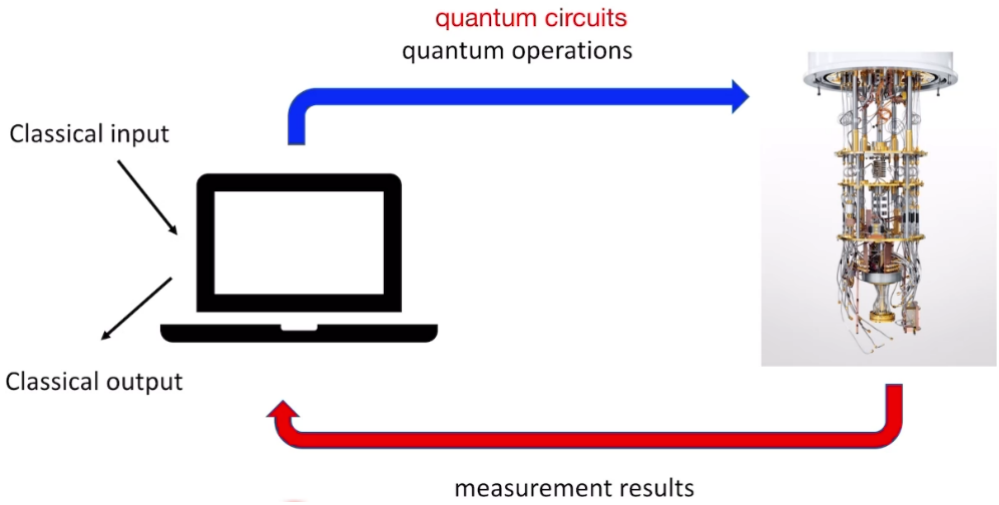


Quantum processor

**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
>
> > $C_n^0$ that outputs 0 if $1^n \notin U$
> > $C_n^1$ that outputs 1 if $1^n \in U$
>
> 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 $C_n^1$.

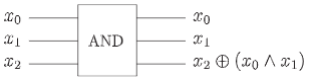
**Uniform Families** So we often impose a **uniformity condition**: the family is uniform if each $C_n$ can be constructed by an appropriately resource-bounded Turing machine. We assume that the circuits can be generated by a Turing machine or equivalent model that on input $n$ produces a description 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 are fundamentally reversible**, per out present understanding: theory of quantum computing is related to a theory of reversible computing **so quantum circuits must be reversible**.

**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}, {AND, XOR, NOT}, {NAND}, {NOR}: NAND and NOR gates have the **functional completeness** property assuming unlimited fanout (a gate can be connected to unlimitedly 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.

## 0.3 Complex Numbers

A field that can be represented in a 2D space.

$$z = a + ib$$

with $a, b \in R$ and $i^2 = -1$, that can be represented in a plot with $Re(z) = a$ on $x$ axis and $Im(z) = b$ on $y$ axis (**cartesian form**).
Can be expressed also as

$$z = \rho(\cos\theta + i\sin\theta) = \rho \cdot e^{i\theta}$$

with $\rho$ being the distance from the origin and $\theta$ the angle (**polar form**). $\rho$ is called modulo and $e^{i\theta}$ is called phase (sometimes referring with that term to just $\theta$)

$$|z|^2 = z \cdot z^* = a^2 + b^2 = \rho^2 = |z^*|$$

$$z^* = \overline{z} = a - ib = \rho(\cos\theta - i\sin\theta) = \rho \cdot e^{-i\theta}$$

with $\overline{z}$ called complex conjugate of $z$.

**Euler Identity** Let's prove the polar form. $e^z$ is a function from $C$ to $C$

$$e^z = \sum_{k=0}^{\infty} = \frac{z^k}{k!}$$

With $z \in C$, let's see with $z = ix$ and $x \in R$. We want to prove that

$$e^{ix} = \cos x + i\sin x$$

$$e^{ix} = \sum_{k=0}^{\infty} \frac{(ix)^k}{k!} = 1 + ix + \frac{i^2x^2}{2} + \frac{i^3x^3}{3!} + \ldots =$$

Let's take the even powers, we have $i^2 = -1, i^4 = +1, \ldots$, and with the odd powers we can take out $i$ from the $\sum$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!} + i \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!} =$$

These are the power series expansions of cos and sin

$$e^{ix} = \cos x + i \sin x$$

This results in the Euler identity which puts together all the principle of math. The imaginary unit an two irrational number together with 1 and 0.

$$e^{i\pi} + 1 = 0 \Leftrightarrow e^{i\pi} = -1$$

**Roots of Unity** Useful when we want to solve $z^n - 1 = 0$. We know that every polynomial has exactly $n$ roots in $C$
Primitive $n$th root of 1

$$\omega_n = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

So for example $\omega_3 = \cos \frac{2}{3}\pi + i \sin \frac{2}{3}\pi = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ for $z^3 - 1 = 0$
So they are counterclockwise on the unitary circle and also unitary roots are cyclic

$$w_n^k = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^k = \cos \frac{2\pi}{n}k + i \sin \frac{2\pi}{n}k = \left(e^{\frac{2\pi i}{n}}\right)^k$$

$\omega_n^0 = 1$

$\omega_n^{n+k} = \omega_n^n \cdot \omega_n^k = \omega_n^k$

$\omega_n^{n-k} = \omega_n^n \cdot \omega_n^{-k} = \omega_n^{-k}$

Multiplication and division are easier in the polar form

$$z_1 \cdot z_2 = \rho_1 \cdot \rho_2(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

$$\frac{z_1}{z_2} = \frac{\rho_1}{\rho_2}(\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2))$$

$$z^n = \rho^n \cdot e^{in\theta}$$

### 0.3.1 Hilbert Spaces

For Quantum Computing only finite dimensional Hilbert spaces meaning complex vector spaces with an inner product.

**Definition** A quantum state space of a system is a vector space (complex) with inner product.
For example, photon polarization: we have a basis and it's a 2-dimensional space. Base states are $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$. We use half-spin patches, $|\uparrow\rangle$ spin up and $|\downarrow\rangle$ spin down.
If we consider a 4-dimensional state space, we have 4 vectors in the base:$|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$ denoted with

$$|v\rangle = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix}$$

using the ket notation.

**Definition** A quantum state is a vector of unitary length in a quantum state space.
So $\||v\rangle\| = 1$, $\|v\| = \sqrt{(v,v)}$ with the inner product defined as

$$(v,w) = \sum_{i=1}^{d-1} v_i^* \cdot w_i$$

We can use the bra

$$\langle v| = (v_0^*, \dots, v_{d-1}^*)$$
$$\langle v \mid w\rangle = (v,w) \in C$$

or the ket-bra

$$|v\rangle\langle w| = (v_i w_j^*)_{i,j}$$

giving a rank-one matrix.

For a system of 1 qubit we have as basis

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

but we can also denote this as $|\uparrow\rangle$ and $|\downarrow\rangle$ and denote as

$$|\rightarrow\rangle = \frac{|\uparrow\rangle + |\downarrow\rangle}{\sqrt{2}}$$

$$|\leftarrow\rangle = \frac{|\uparrow\rangle - |\downarrow\rangle}{\sqrt{2}}$$

as spin-right and spin-left.
We can define spin-in ("in the board")

$$|\otimes\rangle = \frac{|\uparrow\rangle + i|\downarrow\rangle}{\sqrt{2}}$$

and spin-out ("out of the board")

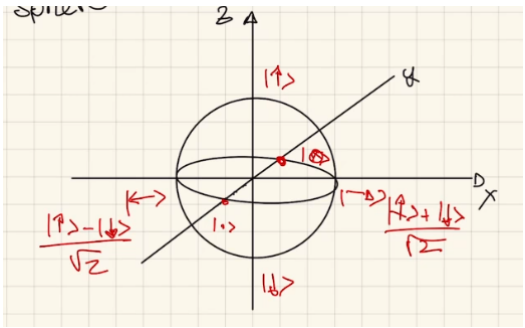
$$|\bullet\rangle = \frac{|\uparrow\rangle - i|\downarrow\rangle}{\sqrt{2}}$$

Multiplying a quantum state bu a global phase ($e^{i\theta}$) we do not change the nature of the quantum state. A global phase is a quantity that multiply all the components of the basis vector.

$$|\rightarrow\rangle = \frac{|\uparrow\rangle + |\downarrow\rangle}{\sqrt{2}} \neq \frac{|\uparrow\rangle + i|\downarrow\rangle}{\sqrt{2}} = |\otimes\rangle$$

In the above case, $i$ is a relative phase.

**Bloch Sphere**



**Pauli Matrices**

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

$$\sigma_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

It reflects the points along the $x$ axis. The same goes for $\sigma_x|1\rangle = |0\rangle$.
So for the points on the $x$ axis stay almost the same.

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

$$\sigma_x|\rightarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

The $y$ axis Pauli matrix is

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

and the last is

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

**Theorem** The three Pauli matrices anticommutes

$$\sigma_i\sigma_j = -\sigma_j\sigma_i$$

for $i, j \in \{x, y, z\}$ and $i \neq j$
Also $\sigma_i^2 = I$

**Hadamard Matrix** Another important matrix, used for building entangled states.

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

It allow to move from the canonical basis to the right-left basis (also known as +- basis).

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

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |\leftarrow\rangle = |-\rangle$$

Also $H^2 = I$, $H^{-1} = H$ so $|0\rangle \mapsto_H |+\rangle$ and $|+\rangle \mapsto_H |0\rangle$ same with $|1\rangle$ and $|-\rangle$, "back and forth".

$$H|\otimes\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}i \end{pmatrix} = |\bullet\rangle$$

**Other common single qubit gates** Already mentioned $X, Y, Z, H$

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

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

**Applying a Gate to a Superposition**

$$\alpha|0\rangle + \beta|1\rangle \mapsto \sigma_x \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \sigma_y \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = -\beta i|0\rangle + \alpha i|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \sigma_z \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto H \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto S \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta i|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \mapsto T \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + e^{i\frac{\pi}{4}}\beta|1\rangle$$

To really play with qubits we introduce **unitary transformations**.

**Unitary Transformations** A unitary transformation is a transformation mapping unit-vectors to unit-vectors. We are interested in some properties of these unitary transformation.
$d$-dimensional quantum state space, it's a vector space so we have a basis: we label the vectors of the base as

$$|0\rangle, |1\rangle, \ldots, |d-1\rangle$$

$$|j\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ with 1 in } j\text{th position}$$

The unitary transformation is $U = [c_0, \ldots, c_{d-1}]$ so we have $U|j\rangle = |c_j\rangle$: $c_j$ is an unit-vector, because $U$ is a unitary transformation:

1. $c_j$ is a unit-vector
   All the columns are unit vectors
2. We can decompose $U$ as sum of rank-1 matrices

$$U = \sum_{k=0}^{d-1} |c_k\rangle\langle k| = |c_0\rangle\langle 0| + |c_1\rangle\langle 1| + \ldots$$

The matrix $|c_i\rangle\langle i|$ for example is of all 0s with $c_i$ in the $i$th column.

$$U|j\rangle = \sum_{k=0}^{d-1} |c_k\rangle\langle k \mid j\rangle = \sum_{k=0}^{d-1} |c_k\rangle\delta_{kj}$$

With $\langle k \mid j\rangle$ inner product $\in C$ and $\delta_{kj} = \begin{cases} 0 & k \neq j \\ 1 & k = j \end{cases}$
We can apply $U$ to combinations, for example

$$U\left(\frac{|k\rangle + |j\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|c_k\rangle + |c_j\rangle)$$

$$\frac{1}{2}(\langle c_k| + \langle c_j|)(|c_k\rangle + |c_j\rangle) = \frac{1}{2}\left(\langle c_k \mid c_k\rangle + \langle c_j \mid c_k\rangle + \langle c_k \mid c_j\rangle + \langle c_j \mid c_j\rangle = 1\right.$$

$\langle c_j \mid c_k \rangle + \langle c_k \mid c_j \rangle \in R$ meaning that $\langle c_j \mid c_k \rangle$ is pure immaginary, $\in C \setminus R$

We can also do with relative phases, for example $i|j\rangle$

$$U\left(\frac{|k\rangle + i|j\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left(|c_k\rangle + i|c_j\rangle\right) = \dots$$

Ending up with the fact that $\langle c_j \mid c_k \rangle$ must be $\in R$.
But we have the same quantity pure immaginary and pure real, meaning that $\langle c_j \mid c_k \rangle = 0$

3. Columns of $U$ are orthogonal and also orthonormal
4. Rows of $U$ are orthonormal ($\Rightarrow$ orthogonal)
5. $U^{-1} = U^H$ **very important**

$$(U^H)_{ij} = u^*_{ji}$$

And $U^H = U^* = U^+$, $U^H$ is the conjugate transpose. Diagonal conjugate, invert triangles and transpose elements. An example with an arbitrary, non unitary, matrix:

$$A = \begin{bmatrix} 1+i & 2-i \\ 3+2i & 4 \end{bmatrix} \Leftrightarrow A^H = \begin{bmatrix} 1-i & 3-2i \\ 2+i & 4 \end{bmatrix}$$

**Spectral Theorem** There are classes of matrices which have an orthonormal basis of eigenvectors, i.e. are diagonalizable by means of orthogonal matrices.
$A = A^T$ symmetric matrices. $\exists$ a orthogonal such that $A = QDQ^T$ with $D$ diagonal matrix with the eigenvalues $\lambda_i$ on the diagonal.
$A = A^H$ hermitan matrices, $AA^H = A^HA$
**Unitary matrices are normal matrices**.
**Spectral theorem**: a matrix $A$ is normal $\Leftrightarrow \exists U$ unitary and $D$ diagonal $\mid A = UDU^H$, meaning that $Au_i = \lambda_i u_i \forall i = 1, \dots, n$, i.e. the columns of $U$ are an orthonormal basis of eigenvectors and $\lambda_i$ are the corresponding eigenvalues.

$$A \in C^{n\times n} = UDU^H = \sum_{k=1}^{n} \lambda_k |u_k\rangle\langle u_k|$$

$$U = [u_1 \mid \dots \mid u_n]$$

$|u_k\rangle\langle u_k|$ is an example of a **orthogonal projector** onto the eigenspace corresponding to $\lambda_k$

**Evaluation of systems**

1. Isolated processes have a unitary evolution
   $|\psi_0\rangle \mapsto |\psi_1\rangle = U_0|\psi_0\rangle \mapsto \dots$
2. From time to time the process is "observed", for example with an experiment: this is called **measurement**.

**Rotations** Of an arbitrary angle $\Theta$ around an axis. Three different rotations, for three different axis.
A rotation is a unitary matrix that can always be expressed $R_x = e^{-i\frac{\Theta}{2}x}$ (example for axis $x$, same for $z$ and $y$)
If $A$ is normal then $A = UDU^H$, so the **exponential of a matrix**

$$e^A = U\left(\sum_{k=1}^{\infty} \frac{D^k}{k!}\right)U^H = Ue^DU^H$$

For example, and since $z$ is diagonal

$$R_z(\Theta) = e^{-i\frac{\Theta}{2}z} = \begin{pmatrix} e^{-i\frac{\Theta}{2}} & 0 \\ 0 & e^{i\frac{\Theta}{2}} \end{pmatrix} = e^{-i\frac{\Theta}{2}}\begin{pmatrix} 1 & 0 \\ 0 & -e^{i\Theta} \end{pmatrix}$$

We get that $R_x(\Theta) = (\cos\frac{\Theta}{2})I - i\sin\frac{\Theta}{2}X$, and in general

$$R_M(\Theta) = \left(\cos\frac{\Theta}{2}\right)I - i\sin\frac{\Theta}{2}M$$

To diagonalize the matrix $\sigma_i$

$$U\sigma_iU^H = D \Rightarrow e^{-i\frac{\Theta}{2}D}$$
$$U^He^{-i\frac{\Theta}{2}D}U = e^{-i\frac{\Theta}{2}\sigma_i}$$

**Theorem** Suppose $U$ is a 1-qubit unitary gate, then there exists real numbers $\alpha, \beta, \gamma, \delta$ such that you can write $U$ like

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

$$\Updownarrow$$

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix}$$

Two rotations around $z$ and one around $y$. Any unitary can be decomposed as a product of three rotations times a phase factor.

**Standard Rotations** The standard rotation gates are those that define rotations around the Pauli matrices $X, Y, Z$ and are defined as

$$R_P(\theta) = e^{-i\theta\frac{P}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) P$$

For the $x$ axis

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

For the $y$ axis

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

For the $z$ axis

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta\frac{P}{2}} & 0 \\ 0 & e^{i\theta\frac{P}{2}} \end{pmatrix}$$

**Tensor Products** Way of putting vectors together to form larger Hilbert/vector spaces.
Let's assume 2 qubits. The state space of these 2 qubits?

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

The state space dimension is 4. Which is the dimension of $n$ qubits? Gives us a state space $2^n$.
$|01\rangle_{AB} = |0\rangle_A |1\rangle_B = |0\rangle_A \otimes |1\rangle_B$ tensor product.

$$\begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} z \\ w \end{pmatrix} = \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$$

With more dimensions

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}$$

For example, $|01\rangle$ encodes 1, meaning "1" in position 1 (counting from 0, so second position)

$$|01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

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

$$I \otimes \sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\sigma_x \otimes I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

**Degrees of freedom** With 1 qubit $\alpha|0\rangle + \beta|1\rangle$ normalized so the constraint $|\alpha|^2 + |\beta|^2 = 1$ and another constraint: we consider the surface of the Bloch sphere of size 2, so $4 - 2 = 2$ degrees of freedom.
With 2 qubits, $2 \cdot 4 - 2$
With $n$ qubits $2 \cdot 2^n - 2 = 2^{n+1} - 2$ degrees

This argument allows us to say that there must be 2-qubit states that cannot be expressed as product of 2 qubits, because the dimensions do not fit.

$$(\alpha|0\rangle_A + \beta|1\rangle_A) \otimes (\delta|0\rangle_B + \gamma|1\rangle_B)$$

You don't get all the possible configurations of 2-qubits. If $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ so the number of qubits in $\psi$ is equal to the sum of the number of qubits in $\psi_1, \psi_2$, then the system is in a **separable state**, otherwise the state is **entangled**. An example of entangled state is the Bell state (EPR state, Einstein Poddsky, Rosen)

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

So no configuration of $\alpha, \beta, \delta, \gamma$ in the previous formula will give the Bell state.

**Inner product of tensor products** Given

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$$

we have that the inner product is

$$\langle \psi \mid \phi \rangle = \sum_{i=0}^{d-1} \psi_i \cdot \phi_i = \langle \psi_1 \mid \phi_1 \rangle \langle \psi_2 \mid \phi_2 \rangle$$

Other properties are

$c(|\psi_1\rangle_A \otimes |\psi_2\rangle) = c|\psi_1\rangle_A \otimes |\psi_2\rangle_B = |\psi_1\rangle_A \otimes c|\psi_2\rangle_B$

$(|\psi_1\rangle_A + |\psi_2\rangle_A) \otimes |\psi_3\rangle_B = |\psi_1\rangle \otimes |\psi_3\rangle_B + |\psi_2\rangle_A \otimes |\psi_3\rangle_B$

$(A \otimes B)(|\psi\rangle_A \otimes |\phi\rangle_B) = A|\psi\rangle \otimes B|\phi\rangle$

$(|\psi\rangle \otimes |\phi\rangle)^* = \langle\psi| \otimes \langle\phi|$

$(A \otimes B)^H = A^H \otimes B^H$

**No Cloning Theorem** We cannot make a copy of an **unknown** qubit.

**Proof** $|\psi\rangle$ unknown qubit in a space of dimension 2, hence $|\psi\rangle|\psi\rangle$ is a space of dimension 4.
$|\psi\rangle|0\rangle$ assumes there exists a $U \mid U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle e^{i\theta}$
$|\phi\rangle|0\rangle$ assumes there exists a $U \mid U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle e^{i\alpha}$

$$(1\langle\psi|\,{}_2\langle 0|)U^H U(|\phi\rangle_1|0\rangle_2) =_1 \langle\psi|\phi\rangle_1\,{}_2\langle 0|0\rangle_2 = \langle\psi|\phi\rangle$$

Because $\langle 0|0\rangle = 1$.
We have $U|\phi\rangle_1|0\rangle = |\phi\rangle|\phi\rangle e^{i\alpha}$ and also $\langle\psi|\langle 0|U^H = (U|\psi\rangle|0\rangle)^H = (|\psi\rangle|\psi\rangle e^{i\theta})$

$$(\langle\psi|\langle\psi|)e^{i(\theta-\alpha)}(|\phi\rangle|\phi\rangle) = \langle\psi|\phi\rangle\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$

But $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \Leftrightarrow \langle\psi|\phi\rangle = 0 \vee \langle\psi|\phi\rangle = 1$
Meaning respectively $|\psi\rangle = |\phi\rangle$ (**equal states**) $\vee$ $|\psi\rangle$ **orthogonal to** $|\phi\rangle$

## 0.4 Quantum Mechanics

QM it's **not a physical theory**, but a **mathematical theory** composed of four postulates describing the behavior of physical systems. We can think of it as an operating system for the universe, users need another layer (physical theories).

### 0.4.1 Four Postulates

**Closed System** A closed/isolated system is an ideal phyisical system that doesn't interact at all with its environment.

1. **Statics**: describes the state of a closed system
2. **Dynamics**: describes the evolution of a closed system
3. **Measurement**: describes how information is extracted from a closed system via interactions with an external system
4. **Composite Systems**: describes the state of a composite system in terms of its component parts.

#### Space-State Postulate

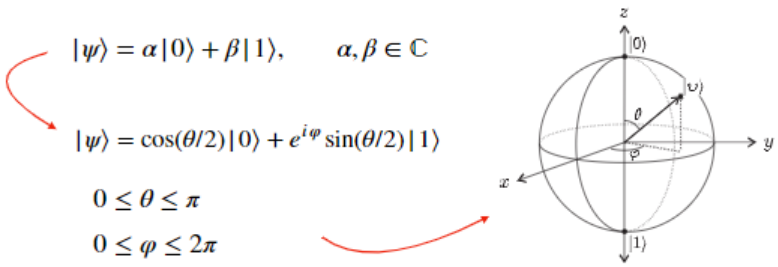
Associated to any physical system there is a **complex Hilbert space known as the state space of the system**. If the system is isolated, then the system is completely described by its state vector, which is a unit vector in the its state space.

**Notes** Tells us that every physical system has a states space, but doesn't tell what the state space is: case-by-case analysis, different physical systems have different state spaces.
Always assuming that the state space is described by a vector in a finite-dimensional complex vector space

**Qubit** Simplest of all isolated quantum systems, which state space is a two-dimensional complex vector space $C^2$ and its state is described by a unit vector $\in C^2$
Any physical system whose state space can be described in $C^2$ can be used to implement a qubit: electrons' spin, photons' polarization...
We've seen $|0\rangle$ and $|1\rangle$, the computational basis states which correspond to $0, 1$ of the classical bits.
We also have the **normalization constraints**

$$\langle \psi \mid \psi \rangle = |\alpha|^2 + |\beta|^2 = 1$$

And we know that we can describe a qubit in two modes: **phase factors**. The global phase factor have no physical significance. Relative phase factors between two orthogonal states in superposition are physically significant: two states that differ for a relative phase factor are physically different and not equivalent.
Qubits can be geometrically represented as a point on the surface of a sphere of unitary radius called **Bloch's Sphere**: geometrical representation of a qubit in 3D space. It's limited in representing a single qubit.




$\theta$ is equivalent to the geometrical latitude: angle with the $z$ axis

$\phi$ is equivalent to the geometrical longitude: angle with the projection on the $(x, y)$ plane and the $x$ axis

#### Evolution Postulate

The time evolution of a closed quantum system is described by the **Schrodinger Equation**

$$ih\frac{d\,|\psi(t)\rangle}{dt} = H(t)\,|\psi(t)\rangle$$

With $h$ being the **Planck's Constant** and $H(t)$ being the **fixed Hermitian operator** known as the Hamiltonian of the system.

**Notes** The postulate describes the evolution of a quantum system in continuous time, with the change described by a differential equation. The Hamiltonian $H(t)$ represent the **total energy** function for the system and tells the quantum state how to change.
If we know the Hamiltonian of a system, then we understand its dynamics completely (at least in principle). In general, figuring it out is very difficult.

**Simplified: Discrete Time Evolution** The discrete time evolution of a closed quantum system is described by a **unitary transformation**. The state $|\psi\rangle$ of the system at time $t_1$ is related to the state $|\psi'\rangle$ at a later time $t_2$ by a unitary matrix $U$ which depends only on the times $t_1$ and $t_2$

$$|\psi'\rangle = U|\psi\rangle$$

This means applying gates one at the time.

**Notes** This expression follows directly form the Schrodinger Equation: every unitary operator $U$ can be realized as a solution of Schrodinger Equation. This postulate, though, doesn't tell us which unitary transformations to use to describe real-world quantum dynamics: case-by-case analysis to figure it out.
Unitary matrices because they preserve length.

**Measurements** We postulate that closed quantum systems evolve according to a unitary operator. We will be interested in observing and **measuring** some properties of a system: at some point we must allow the system to interact with the measurement apparatus, making the system no longer closed and the Evolution Postulate no longer appropriate.
The evolution of the state of a system during a measurement is not unitary: the third postulate provides a means for describing the effects of measurements on quantum systems.
Quantum Systems do get perturbed and modified, and only the probability of observing specific values can be calculated: measurement is a non-deterministic process.

**Measurement Postulate**

Quantum measurements are described by a collection $\{M_m\}$ of measurements operators that satisfy the **completeness relation**

$$\sum_m M_m^+ M_m = I$$

$m$ labels the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then for each $m$:

The probability that result $m$ occurs is given by

$$p(m) = \langle\psi|M_m^+ M_m|\psi\rangle = \|M_m\,|\psi\rangle\|^2$$

The state of the system after the measurement with outcome $m$ is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^+ M_m|\psi\rangle}}$$

**Notes** This is only a mathematical formalism for measurements. The state of the system after the measurement is a properly normalized quantum state, and in general it is not a scalar multiple of $|\psi\rangle$: the measurement has modified the state of the system.
The denominator vanishes only if $p(m) = 0$, meaning that the result $m$ will never occur.
The completeness equation expresses the fact that probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^+ M_m|\psi\rangle = \langle\psi|I|\psi\rangle = \langle\psi|\psi\rangle = 1$$

**Example**

**Projective Measurements** For many applications of quantum computation and quantum information we will mostly perform **projective measurements**, as subset of the possible measurements.
Defined in terms of the Hermitian operator: an operator $M$ is Hermitian if it's self-adjoint: $M^+ = M$
In physics, Hermitian operators are called observable: **an observable is a property of a physical system that can be measured** (position, polarization...), and to each physical observable there corresponds an Hermitian operator.
All eigenvalues of an observable (so of an Hermitian operator) are real, and the eigenvectors are orthogonal. The **possible outcomes of a measurement correspond to the eigenvalues of the observable** $M$.
Observables can be thought of as questions we can pose to quantum systems: each question admits a set of answers, the eigenvalues of the observable.

Any observable $M$ can be written as its **spectral decomposition**

$$M = \sum_m P_m = \sum_m m|u_m\rangle\langle u_m|$$

$m$ are the real eigenvalues of $M$ (outcomes)

$|u_m\rangle$ is the eigenvector associated to $m$

$P_m = |u_m\rangle\langle u_m|$ is the **projector** onto the eigenspace of $M$ with real eigenvalue $m$

Projectors are operators $P$ which satisfy $P^2 = P$
An example is the operator $|0\rangle\langle 0|$

$$(|0\rangle\langle 0|)^2 = |0\rangle\langle 0||0\rangle\langle 0| = |0\rangle\ (\langle 0|0\rangle)\ \langle 0| = |0\rangle\langle 0|$$

since $\langle 0|0\rangle = 1$

**Example**

**Expectation**

$$E_\psi[M] = \langle\psi|M|\psi\rangle$$

**Recap on Measurement Postulate** It's a mathematical formalism for measurements. It doesn't tell us what measurement can be done in practice or with what efficiency. Some measurements can be simple to state mathematically but **not easy to implement**.
Tells us how to compute the probability $P(m)$ that outcome $m$ occurs and the new state of the system after the measurement with outcome $m$ applying the measurement operators $M_m$ (one operator for each possible outcome).
For projective measurement, these operators, can be derived from the spectral decomposition of the observable $M$ corresponding to the measurement.
An observable is a property of a physical system (a **physical quantity**) that can be measured: position, polarization... Each physical observable corresponds to a **Hermitian operator**, all eigenvalues of an observable are real and the eigenvectors are orthogonal. The **possible outcomes of a measurements are the real eigenvalues of** $M$.
Any observable $M$ can be written it as its **spectral decomposition**

$$M = \sum_m mP_m = \sum_m m|u_m\rangle\langle u_m|$$

where

$m$ are the real eigenvalues, the outcomes of the measurements

$|u_m\rangle$ is the eigenvector associated to $m$

$P_m = |u_m\rangle\langle u_m|$ is the **projector** onto the eigenspace of $M$ with real eigenvalue $m$

The measurement operators are the projectors $P_m = |u_m\rangle\langle u_m|$
The probability of getting result $m$ on the state $|\psi\rangle$ is

$$p(m) = \langle\psi \mid P_m^+ P_m \mid \psi\rangle = \langle\psi|P_m|\psi\rangle$$

Given that outcome $m$ occurred, the state of the quantum system immediately after is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$$

The operators $P_m$ satisfy the completeness relation.

$$\sum_m P_m^+ P_m = \sum_m P_m = I$$

**Measurements in the Standard Basis** A measurement in the $|0\rangle, |1\rangle$ basis corresponds to perform a projective measurement with projectors

$$P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1//0 \end{pmatrix} (1\ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 1//0 \end{pmatrix} (1\ 0) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Can be seen as projective measurement with respect to Hermitian matrix $Z$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Or also with respect to $I$ with eigenvalues equal to 1

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

**Measurements in Orthonormal Basis** A measurement in an orthonormal basis $\{|m\rangle\}$ corresponds to perform a projective measurement with projector operators

$$P_m = |m\rangle\langle m|$$

For example in the hadamard basis $|+\rangle, |-\rangle$

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

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

Corresponds to perform projective measurement with projectors

$$P_+ = |+\rangle\langle +| = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} (1\ 1) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$P_- = |-\rangle\langle -| = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} (1\ -1) = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

And the completeness equation is satisfied

$$P_+^+ P_+ + P_-^+ P_+ = P_+ + P_- = I$$

Single qubit measurements: measuring the identity but also measures the projection over the $x$ axis. All Pauli matrices have eigenvalues of +1 and -1:

$$X = |+\rangle\langle +| - |-\rangle\langle -| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

**Measuring example** Measuring the state

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

in the $|+\rangle, |-\rangle$ basis gives the result + with probability

$$P(+) = \langle\psi|P_+|\psi\rangle = \langle\psi|+\rangle\langle +|\psi\rangle = \frac{1}{2}|\alpha + \beta|^2$$

and state after the measurement is $|+\rangle$, while it gives the result $-$ with probability

$$P(-) = \langle\psi|P_-|\psi\rangle = \langle\psi|-\rangle\langle -|\psi\rangle = \frac{1}{2}|\alpha - \beta|^2$$

and state after is $|-\rangle$.
Also relative phase factors are important. Consider the state $|+\rangle, |-\rangle$ differing just for a relative phase factor (plus and minus)

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

We cannot distinguish between them by measuring in the computational basis: both 0,1 outcomes occur with probability $\frac{1}{2}$.
Considering the $|+\rangle, |-\rangle$ basis, which has measurements operators $P_+, P_-$ if we measure the state $|+\rangle$ we always get outcome $+$, $P(+) = 1, P(-) = 0$. Opposite for measuring $|-\rangle$ getting always $-$ as outcome. So measuring in the $|+\rangle, |-\rangle$ basis distinguish the two state perfectly, relative phase matters.
How to measure in a basis different from the computational basis? In the computational basis we have a register, quantum information becomes classical information. How to measure in different basis, for instance the hadamard basis?
First we apply a change of basis from the hadamard back to the computational. Then measure respect to the computational and after we change back to the original basis. Example We measure either $|0\rangle$ or $|1\rangle$, how to change back? Just apply again the change of basis transformation, since the circuits are always reversible.
In general, to implement a measurement with respect to an orthonormal basis $\{\phi_j\rangle\}$:

The matrix $U$ is applied to perform a basis change to the computational basis

$$U\left(\sum_j \alpha_j|\phi_j\rangle\right) = \sum_j \alpha_j U|\phi_j\rangle = \sum_j \alpha_j|j\rangle$$

Then a measurement is made in the computational basis obtaining a specific (classical) outcome with probability $|\alpha_j|^2$.
The state of the system after this measurement is $|j\rangle$

Finally $U^{-1}$ is applied to change back to the $\{|\phi_j\rangle\}$ basis, leaving the post-measurement state $|\phi_j\rangle$

**Composition of Systems**

The **state space of a composite physical system is the tensor product of the state spaces of the component subsystems**. Moreover, if we have systems numbered 1 through $n$, and system number $i$ is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is

$$|\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$$

Often $\otimes$ is omitted and the above formula is rewritten as $|\psi_1, \ldots, \psi_n\rangle$
Tensor product is the mathematical structure used to describe the state space of a composite physical system because we need a new space which captures the interaction of all $n$ systems.
Not all states of acombined system can be separated into the tensor product of states of the individual components.
Notation:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|\phi\rangle = \gamma|0\rangle + \delta|1\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

**Joint state of the two qubits**

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

**Standard basis notation**

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

**Separable States** A state $|\psi\rangle \in C^n \otimes C^m$ of a combined system is a **separable state** if it can be expressed as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in C^n$ and $|\psi_2\rangle \in C^m$
For example

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

For example we get separable state when qubits are prepared independently and kept isolated.
Physical separation does not imply that the joint state must be separable. Two physically separated particles can be entangled (correlated).

**Entangled States** A state of a composite system that cannot be written as a product of states of its component systems is called **entangled state**.
For example the bell state is entangled, cannot be writted as a product of single-qubit states:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Either $\alpha$ or $\delta$ must be zero but with alpha zero the first element is zero, with delta zero the last element is zero. Cannot exist.

**Example** 2 qubit composite system $|\psi_1\rangle \otimes |\psi_2\rangle$ where we apply the $X$ (NOT) gate only to the first qubit. So implicitly we apply the identity gate $I$ to the second qubit.

$$|\psi_1\rangle \otimes |\psi_2\rangle \mapsto X|\psi_1\rangle \otimes I|\psi_2\rangle = (X \otimes I)(|\psi_1\rangle \otimes |\psi_2\rangle)$$

So for a $n$ qubit composite system $|\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$, applying the $X$ gate to the first qubit corresponds to applying the operation $X \otimes I \otimes \ldots \otimes I$ (with $I$ repeated $n-1$ times) to the entire system.

**CNOT Gate** Just as there are 2-qubit states that cannot be written as the product of two 1-qubit states, there are 2-qubit gates (acting on both qubits) that cannot be written as a tensor product of two 1-qubit gates.
The CNOT gate flips the state of the second qubit if the first qubit is in state $|1\rangle$, and does nothing otherwise:

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

Represented as a matrix:

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

and **cannot be written as a tensor product of two 1-qubit gates**.

**Measurements on Multiple Qubits** Considering a two qubit state

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

a complete set of measurement operators in the computational basis would be

$$P_{00} = |00\rangle\langle 00| \;\; P_{01} = |01\rangle\langle 01| \;\; P_{10} = |10\rangle\langle 10| \;\; P_{11} = |11\rangle\langle 11|$$

When measuring the two qubits we get

the result 00 with probability $|\alpha|^2$

the result 01 with probability $|\beta|^2$

the result 10 with probability $|\gamma|^2$

the result 11 with probability $|\delta|^2$

How do we measure only the first qubit? We **tensor the desired measurement operator with the identity matrix**: if we measure the first qubit to be in state $|0\rangle$, the measurement operator will consist of projectors onto the state $|00\rangle, |01\rangle$ since we must consider all states consistent with the measurements.

$$P_{0*} = |00\rangle\langle 00| + |01\rangle\langle 01| = (|0\rangle \otimes |0\rangle)(\langle 0| \otimes \langle 0|) + (|0\rangle \otimes |1\rangle)(\langle 0| \otimes \langle 1|) =$$
$$= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| = |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) = |0\rangle\langle 0| \otimes I$$

because $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$. Similarly

$$P_{1*} = |10\rangle\langle 10| + |11\rangle\langle 11| = \ldots = |1\rangle\langle 1| \otimes I$$

Therefore the probability of measuring the first qubit in state $|0\rangle$ is

$$p(0) = \langle\psi|P_{0*}|\psi\rangle = \langle\psi|\,|0\rangle\langle 0|\otimes I|\psi\rangle = (\alpha* \;\beta* \;\gamma* \;\delta*)\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\\\gamma\\\delta\end{pmatrix} = (\alpha* \;\beta* \;\gamma* \;\delta*)\begin{pmatrix}\alpha\\\beta\\0\\0\end{pmatrix} = |\alpha|^2+|\beta|^2$$

As expected $p(0)$ is the sum of the probabilities of measuring $|00\rangle$ and $|01\rangle$.
The state after the measurement is

$$\frac{P_{0*}|\psi\rangle}{\sqrt{p(0)}} = \frac{1}{\sqrt{|\alpha|^2+|\beta|^2}}(|0\rangle\langle 0|\otimes I)(\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle) = \frac{1}{\sqrt{|\alpha|^2+|\beta|^2}}(\alpha|00\rangle+\beta|01\rangle)$$

The relative probability of observing $|00\rangle$ and $|01\rangle$ hasn't changed, but by measuring $|0\rangle$ on the first qubit we have eliminated the possibilities that the system is in either the state $|10\rangle$ or $|11\rangle$

**Example** Given

$$|\psi\rangle = \sqrt{\frac{1}{11}}|00\rangle + \sqrt{\frac{5}{11}}|01\rangle + \sqrt{\frac{2}{11}}|10\rangle + \sqrt{\frac{3}{11}}|11\rangle$$

Then the probability of measuring 0 in the first qubit is $\frac{1+5}{11} = \frac{6}{11}$ and the state after measuring it becomes

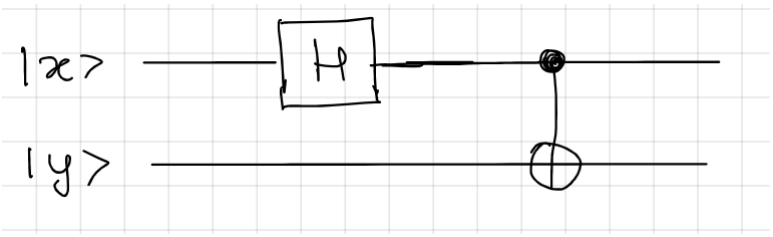
$$\sqrt{\frac{11}{6}}\left(\sqrt{\frac{1}{11}}|00\rangle + \sqrt{\frac{5}{11}}|01\rangle\right)$$

### 0.4.2 Superdense Coding

Simple yet surprising application of elementary quantum mechanics. It involves two parties, Alice and Bob, who are far away from each other and the goal is the following: Alice in in possession of two classical bits of information which she wishes to send to Bob **using a single qubit**.
Alice and Bob initially share a pair of qubits in the entangled Bell state

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

One qubit is in Alice's possession, the other is in Bob's possession.
How are the Bell states formed?




$$|00\rangle \to H\otimes I \to \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle \to \text{CNOT} \to \frac{|00\rangle+|11\rangle}{\sqrt{2}} = |\beta_{00}\rangle$$

$$|01\rangle \to H\otimes I \to \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle \to \text{CNOT} \to \frac{|01\rangle+|10\rangle}{\sqrt{2}} = |\beta_{01}\rangle$$

$$|10\rangle \to H\otimes I \to \frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle \to \text{CNOT} \to \frac{|00\rangle-|11\rangle}{\sqrt{2}} = |\beta_{10}\rangle$$

$$|11\rangle \to H\otimes I \to \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle \to \text{CNOT} \to \frac{|01\rangle-|10\rangle}{\sqrt{2}} = |\beta_{11}\rangle$$

**Every vector is this basis is entangled!**

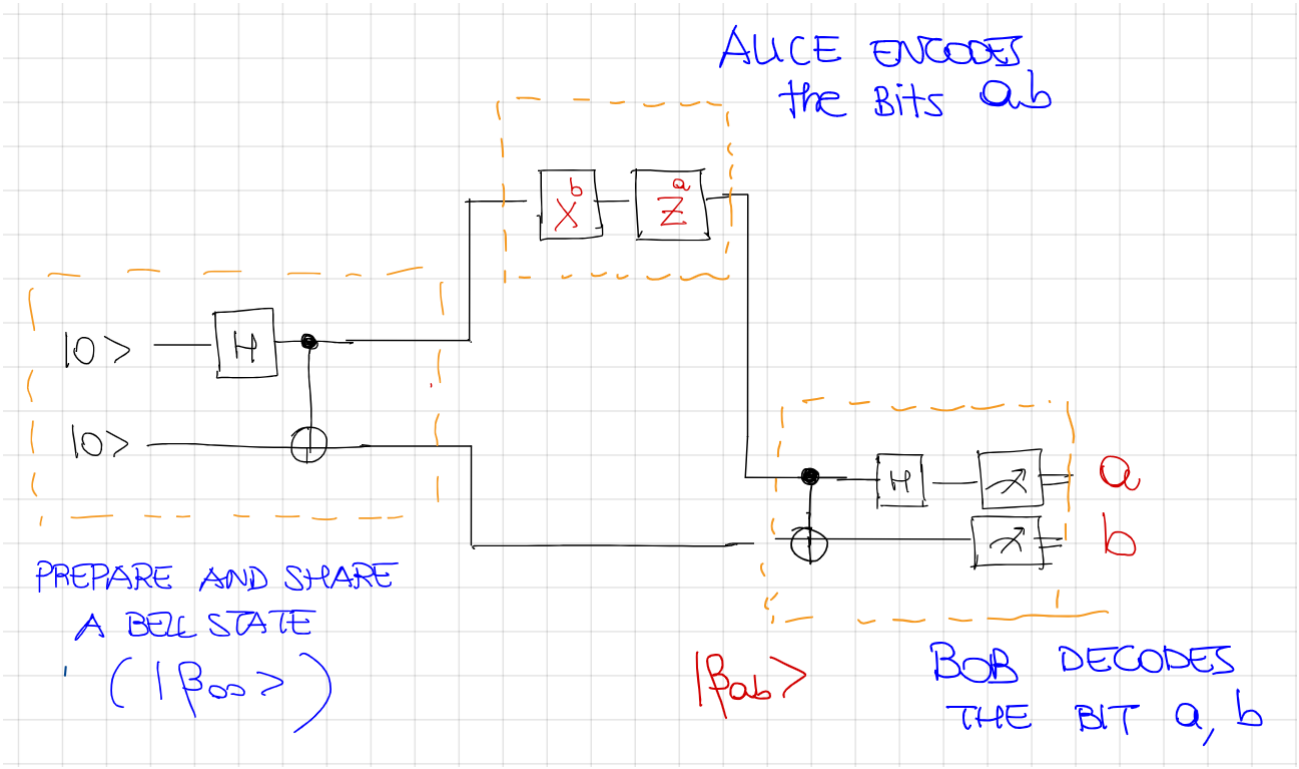
**Sharing a Pair of Entangled Bits**

The state $|\beta_{00}\rangle$ would have to be created ahead of time, when the qubits are in a lab together and can be made to interact in a way that will give rise to the entanglement between them.

After the state is created, Alice and Bob each take one of the two qubits away with them.

Alternatively, some third party may prepare the entangled state ahead of time and sens one qubit to Alice and the other to Bob.

If they are careful not to let the qubits interact with the environment or other quantum systems, Alice and Bob's joint state will remain entangled.
Note that $|\beta_{00}\rangle$ is a fixed state, there is no need for Alice to have sent any qubit to Bob to prepare this state.




**Procedure**

| To send | Alice applies to her qubit the gate | Resulting state |
|---|---|---|
| 00 | $I$ | $\|\beta_{00}\rangle \mapsto \|\beta_{00}\rangle$ |
| 01 | $X$ | $\|\beta_{00}\rangle \mapsto \frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\beta_{01}\rangle$ |
| 10 | $Z$ | $\|\beta_{00}\rangle \mapsto \frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\beta_{10}\rangle$ |
| 11 | $ZX$ | $\|\beta_{00}\rangle \mapsto_{X\otimes I} \frac{\|10\rangle+\|01\rangle}{\sqrt{2}} \mapsto_{Z\otimes I} \frac{-\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\beta_{11}\rangle$ |

The resulting state is one of the four Bell states, which form an orthonormal basis and can be distinguished by an appropriate quantum measurement. So after applying the appropriate gate, Alice sends her qubit to Bob. Bob is in possession of one of the four Bell states, depending on the classical bits that Alice wished to send him, so he performs a measurement in the Bell basis and determines which bit string Alice sent.
The measurement can be implemented by first performing a change of basis, then performing a measurement in the computational basis.
The outcome of the Bell measurement reveals to Bob the Bell states he possesses and allows him to determine with certainty the two classical bits.
The measurement gives Bob the values $a, b$ corresponding to the Bell state $|\beta_{ab}\rangle$ in his possession.

**Example** Alice wants to send 10, so she applies $Z$ to her qubit

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \mapsto_{Z\otimes I} \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

and send the qubit to Bob. Bob performs the measurement: applies a CNOT with the first qubit as control and the second as target, then a Hadamard on the first:

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} \mapsto_{\text{CNOT}} \frac{|00\rangle - |10\rangle}{\sqrt{2}} \mapsto_{H\otimes I} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle\right) =$$

$$= \frac{1}{2}(\cancel{|00\rangle} + |10\rangle - \cancel{|00\rangle} + |10\rangle) = \frac{1}{2}(2|10\rangle) = |10\rangle$$

Now Bob has the state $|10\rangle$ and know that Alice sent 10.

Alice, interacting with only a single qubit, is able to transmit two bits of information to Bob. Two qubits are involved in the protocol, but Alice never need to interact with the second qubit. Classically, the task Alice accomplishes would have been impossible had she only transmitted a single classical bit.
Information is physical, and surprising physical theories as Quantum Mechanics may predict surprising information processing abilities.

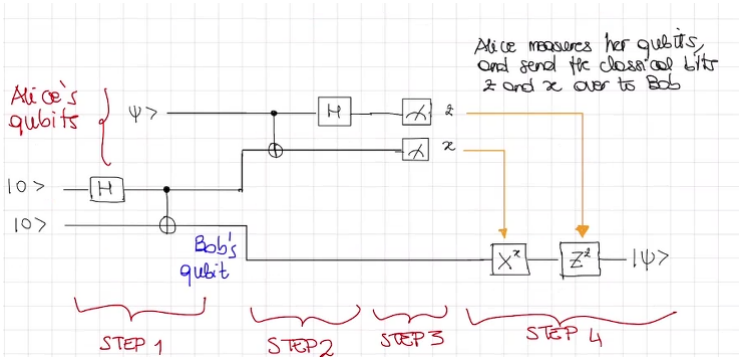
**Communication Channels**

> **Quantum Communication Channel** is a communication line (e.g. fiber optic, cable...) which can carry qubits between two remote locations.
>
> **Communication Channel** is a line that can carry only classical bits (and not qubits).

**Quantum Teleportation** Process by which a quantum state is transfered from one location to another, without sending directly the quantum state.
Alice has $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and would like to send the quantum state to Bob.

> Alice could physically send the qubit but we rule out this possibility because we want to "teleport".
>
> Alice could tell Bob the amplitude $\alpha$ and $\beta$ for the quantum state $|\psi\rangle$. To do this, she doesn't need to send a quantum state, but she can simply send the complex numbers $\alpha$ and $\beta$ as ordinary classical information e.g. over the internet. Bob could then re-create the state in his lab.
> But **in general Alice doesn't know the identity of her quantum state**.

**Quantum teleportation works even when the identity of a the state isn't known to Alice or Bob**. The teleportation instead works like this. The circuit is:




Alice has two qubits, Bob just one.

> **Step 1**: two qubits are prepared entangled and shared.
>
> **Step 2**: Alice lets the two qubits interact and measure with a Bell basis measurement, basically by changing the base.
>
> **Step 3**: Alice measures her two qubits in the computational basis. She has 4 possible equiprobable outcomes.
>
> **Step 4**: Bob receives the two classical bits from Alice and restores the state $|\psi\rangle$ on his qubit.

No particle have been sent from Alice to Bob, just two classical bits used by Bob to recover the state $|\psi\rangle$. Moving is possible, copying is not possible: $|\psi\rangle$ is not in possession of Alice anymore.
Alice measures in the Bell state because: after step one we have $|\psi\rangle|\beta_{00}\rangle$ and you can prove that this is equal to

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{2}(|\beta_{00}\rangle|\psi\rangle + |\beta_{01}\rangle X|\psi\rangle + |\beta_{10}\rangle Z|\psi\rangle + |\beta_{11}\rangle XZ|\psi\rangle)$$

## 0.5 Quantum Algorithms

The really important question is when quantum computers can outperform classical ones.
With a

$$f : \{0,1\} \to \{0,1\}$$

we have 4 functions

| | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 |

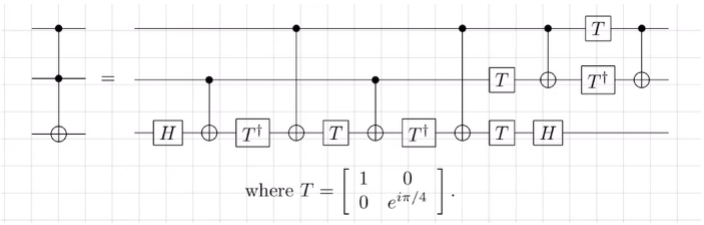
With classical algorithms we need two queries to see if a function is balanced or constant. In quantum algorithms we need to query the oracle only once because we can exploit quantum parallelism. Feed the circuit with a superposition of inputs and the oracle returns a superposition of outputs. This is the **Deutsch algorithm**, and the **Deutsch problem** is the following: given a black box for computing an unknown function $f : \{0,1\} \to \{0,1\}$, determine if the function is balanced or constant by making queries to $f$.

### 0.5.1 Classical Computations on Quantum Computers

We want to compute functions

$$f : \{0,1\}^n \to \{0,1\}$$

We need to have a **reversible computation**, so unitary gates: can't feed the entire input sequence into a gate. We take any classical logic circuits computing out function, than change each gate into a reversible version. Once we have a computable function with reversible gate than we can translate it into a quantum ambient.
To translate a gate into a reversible version we use Toffoli gates, which are reversible versions of the AND. Toffoli gates are C-CNOT. With $C = 0$ is AND, with $C = 1$ is a NAND.
Toffoli gate and the quantum implementation:

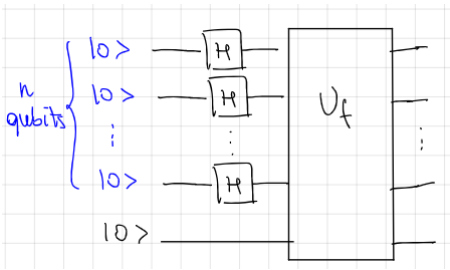



Any classical computation can be implemented by a quantum circuit of Toffoli gates.

**Quantum Parallelism** An oracle computing a function is a black-box that computes said function. Quantum if used with quantum bits.
$U_f$ is implemented, due to reversibility, with input $|x\rangle$ of size $n$ and another qubit $|y\rangle$ used to store the result. The output is $|x\rangle$ and $|y \otimes f(x)\rangle$. It's reversible

$$|x, y\rangle \mapsto_{U_f} |x, y \otimes f(x)\rangle \mapsto_{U_f} |x, (y \otimes f(x)) \otimes f(x)\rangle = |x, y\rangle$$

In general $|x\rangle$ is of size $n$, meaning $f : \{0,1\}^n \to \{0,1\}$. To prepare the $|x\rangle$ (data register) in a superposition we apply the Hadamard gate, and we can generalize this procedure on an arbitrary number of qubits:




So we:

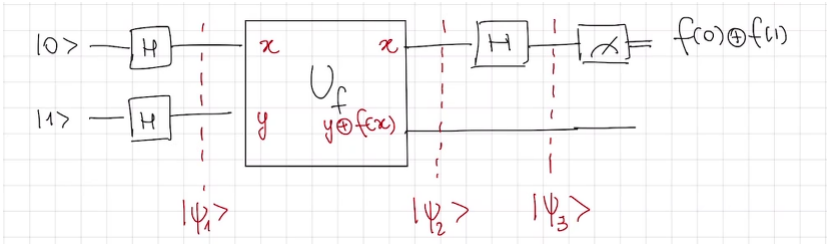
Prepare the $n + 1$ qubit state $|x\rangle^{\otimes n}|y\rangle$

Apply the $H$ gate to the first $n$ qubits, to obtain the equal superposition of all inputs of $f$

Apply the quantum circuit implementing $U_f$

Obtaining the state $\frac{1}{\sqrt{2^n}}\sum_x |x, f(x)\rangle$
Quantum parallelism enables all possible values of $f$ to be evaluated simultaneously, even if we evaluate $f$ once. This parallelism is not immediately useful: if we measure the state $\frac{1}{\sqrt{2^n}}\sum_x |x, f(x)\rangle$ we obatin $|x, f(x)\rangle$ for a single value of $x$.
To exploit quantum parallelism, we need the ability to extract information about more than one value of $f(x)$ from $\sum_x |x, f(x)\rangle$

### 0.5.2 Deutsch's Algorithm




$$f(0) \otimes f(1) = \begin{cases} 0 & f \text{ is constant} \\ 1 & f \text{ is balanced} \end{cases}$$

This circuit solves Deutsch's problem in just one pass. The Hadamard gate on the state $|1\rangle$ is to let the amplitude interfere in order to grasp global properties of the function. The last part measures in the Hadamard basis.

$$|\psi_1\rangle = |+\rangle|-\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$$

Recall that the oracle $U_f$ works like this

$$|x\rangle|-\rangle = |x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \mapsto_{U_f} |x\rangle\frac{|0\oplus f(x)\rangle-|1\otimes f(x)\rangle}{\sqrt{2}} = |x\rangle\frac{|f(x)\rangle-|\overline{f(x)}\rangle}{\sqrt{2}} = \begin{cases} |x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} = |x\rangle|-\rangle & f(x)=0 \\ |x\rangle\frac{|1\rangle-|0\rangle}{\sqrt{2}} = -|x\rangle|-\rangle & f(x)=1 \end{cases}$$

With $\overline{x}$ being the complement of $x$ (if $x = 0$ then $\overline{x} = 1$)
So the state doesn't change with $f(x) = 0$ and has a phase factor with $f(x) = 1$. A more compact way is $(-1)^{f(x)}|x\rangle|-\rangle$

So we have

$$|\psi_2\rangle = U_f(|+\rangle|-\rangle) = U_f\left(\frac{|0\rangle|-\rangle}{\sqrt{2}} + \frac{|1\rangle|-\rangle}{\sqrt{2}}\right) = \frac{(-1)^{f(0)}|0\rangle|-\rangle + (-1)^{f(1)}|1\rangle|-\rangle}{\sqrt{2}} = \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}|-\rangle =$$

$$= \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}}|-\rangle = \pm|+\rangle|-\rangle & f \text{ is constant and } f=0 \text{ or } 1 \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}}|-\rangle = \pm|-\rangle|-\rangle & f \text{ is balanced and } f(0)=0, f(1)=1 \text{ or viceversa} \end{cases}$$

Then we apply Hadamard on the first qubit

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle = \begin{cases} \pm(H|+\rangle)|-\rangle & f \text{ is constant} \\ \pm(H|-\rangle)|-\rangle & f \text{ is balanced} \end{cases} = \begin{cases} \pm|0\rangle|-\rangle & f \text{ is constant} \\ \pm|1\rangle|-\rangle & f \text{ is balanced} \end{cases}$$

With a measure on the computational basis we solve the Deutsch's problem, getting $0 \Leftrightarrow f$ is constant and $1 \Leftrightarrow f$ is balanced.

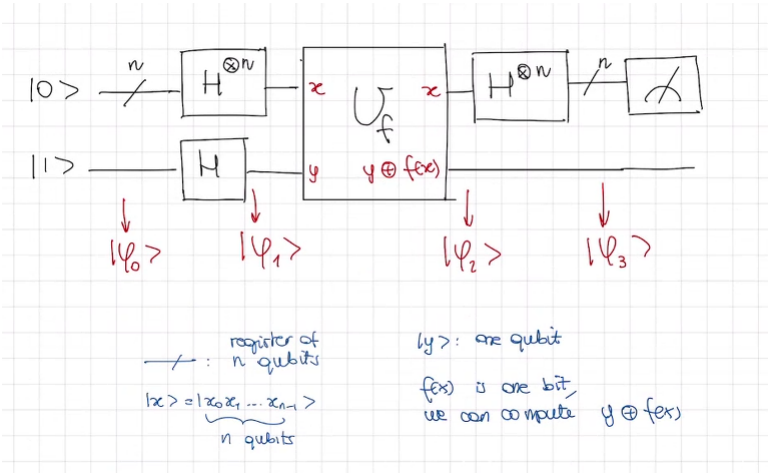
### 0.5.3 Deutsch-Jozsa Algorithm

Generalization of the Deutsch's problem

$$f : \{0,1\}^n \to \{0,1\}$$

As input we have a black box for computing an unknown function $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced. The problem is to determine whether $f$ is constant or balanced.

Classical (exact) solution, in the best case we query twice getting two different answers, then $f$ is balanced for sure. The worst case is $2^{n-1}$ queries with the same result, so $2^{n-1} + 1$ queries: if the last value is different then is balanced, otherwise is constant. So classically we need an exponential number of queries. With quantum circuits we do just one query.




Very similar, just with a $n$ qubits on state $|0\rangle$ in the query register and 1 qubit in state $|1\rangle$ in the answer register.

$$|\psi_0\rangle = |0\dots0\rangle|1\rangle = |0\rangle^{\otimes n}|1\rangle$$

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2}}|-\rangle$$

Query register: uniform superposition of all values.
Answer register: uniform superposition of state $|0\rangle$ and $|1\rangle$.

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}U_f\left(\sum_{x\in\{0,1\}^n}|x\rangle|-\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}U_f(|x\rangle|-\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle$$

Let's see on a single qubit

$$H|x_i\rangle = \frac{|0\rangle+(-1)^{x_i}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\sum_{z_i\in\{0,1\}}(-1)^{x_i}|z_1\rangle = \begin{cases} \frac{1}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} & x_i = 0 \\ \frac{1}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} & x_i = 1 \end{cases}$$

So we have

$$H^{\otimes n}|x\rangle = (H|x_0\rangle)\dots(H|x_{n-1}\rangle) = \frac{1}{\sqrt{2}}\left(\sum_{z_0=0}^{1}(-1)^{x_0z_0}|z_0\rangle\right)\dots\left(\sum_{z_{n-1}=0}^{1}(-1)^{x_{n-1}z_{n-1}}|z_{n-1}\rangle\right) =$$

$$= \frac{1}{\sqrt{2^n}}\sum_{z_0=0}^{1}\dots\sum_{z_{n-1}=0}^{1}(-1)^{x_0z_0+\dots+x_{n-1}z_{n-1}}|z_0\rangle\dots|z_{n-1}\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle$$

So

$$|\psi_3\rangle = H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(x)}|x\rangle\right)|-\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_x(-1)^{f(x)}H^{\otimes n}|x\rangle\right)|-\rangle =$$

$$= \frac{1}{\sqrt{2^n}}\left(\sum_x(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle\right)|-\rangle = \frac{1}{2^n}\sum_{z\in\{0,1\}^n}\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot z}|z\rangle\right)|-\rangle$$

Let's consider the amplitude of the state $|z\rangle = |0\dots0\rangle$

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+0} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = \begin{cases} -1 & f \text{ is constant and } = 0 \\ +1 & f \text{ is constant and } = 1 \\ 0 & f \text{ is balanced} \end{cases}$$

So if $f$ is constant, the amplitude of $|0\dots0\rangle$ is $\pm1$ (all other amplitudes are 0 since $|\psi_3\rangle$ is a unit vector), and a measurement in the computational basis is certain to return all zeroes (the binary string $0\dots0$).
If $f$ is balanced, positive and negative contributes cancel each other and the overall amplitude is 0, the measurement is certain not to return all zeroes.

**Probability Error**

$$2\left(\frac{1}{2}\right)^k = \frac{1}{2^{k-1}}$$

**Simon's Algorithm**

$$f : \{0,1\}^n \to \{0,1\}^n$$

Is $f$ one-to-one (bijection) or two-to-one function?

### 0.5.4 Quantum Fourier Transform

Building block for many important algorithms: QPE, QAA, Shor's, QS...

**Discrete Fourier Transform** DFT, essentially multiplying a unitary matrix by a vector. With Fast Fourier Transform we do it in $O(N \log N)$ with $N = 2^n$.
We have $x_0, \dots, x_{N-1}$ and $y_0, \dots, y_{N-1}$ Primitive root of unity $\omega_N = e^{\frac{2\pi i}{N}}$

$$y_N = \frac{1}{\sqrt{N}} = \sum_{j=0}^{N-1} e^{\frac{2\pi i j k}{N}} x_j = \sum_{j=0}^{N-1} \omega_N^{jk} x_j$$

So we have

$$y = F_N x$$

with $F_N$ unitary matrix, given by the $k$ indexes. $k = 0$ we have all ones in the first row.

$$F_n = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & \dots & \dots & 1 \\ 1 & w_N & \dots & \omega_N^{N-1} \\ \vdots & & & \\ 1 & & & \end{bmatrix}$$

$$w_N^{kj} \text{ in positions } k, j = 0, \dots, N-1$$

The conjugation of $w_N^{jk}$ is $\cos \pm i \sin$ changing the sign.

$$F_N \cdot F_N^H = \frac{1}{N} \left[ \ w_{kj} \ \right] \left[ \ w_{sp}^{-1} \ \right] =$$

$F_N$ needs to be unitary so this multiplication must be $I$, so $(F_N \cdot F_N^H)_{st} = \begin{cases} 0 & s \neq t \\ 1 & s = t \end{cases}$

It's provable that $\sum_{j=0}^{N-1} \omega_N^{kj} = \begin{cases} N & k = 0 \bmod N \\ 0 & k \neq 0 \bmod N \end{cases}$
So essentially we have

$$(F_N F_N^H)_{st} = \frac{1}{N} \sum_{j=0} \omega_N^{js} \omega_N^{-jt} = \frac{1}{N} \sum_{j=0}^{N-1} \omega_N^{j(s-t)}$$

So it's unitary

**Example** $n = 1, N = 2$

$$F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$$

$$\omega_2 = \cos \pi + i \sin \pi$$

**Quantum Fourier Transform** We're in the quantum world, so we're working with quantum states. When we measure we collapse from a state, losing the superposition.
$|y\rangle = H^{\otimes n}|x\rangle$ is already a quantum Fourier transform, over a group $Z_2 \otimes Z_2 \otimes \ldots \otimes Z_2$, binary.
Thanks to Coppersmith in 1994, we pass from $O(N \log N) = O(2^n n)$ of the fast (classical) Fourier transform to the $O(n^2)$ of the quantum one, so from exponential to polynomial: an exponential speedup. But they don't compute the same quantities.

We define QFT on an orthonormal basis

$$|0\rangle, |1\rangle \ldots |N-1\rangle$$
$$|\tilde{j}\rangle = QFT(|j\rangle)$$

More in general, with

$$x = \sum_{j=0}^{N-1} x_j |j\rangle$$
$$|\tilde{x}\rangle = QFT(|x\rangle)$$

To define, we start from the classical definition applying to each element of the basis

$$|\tilde{j}\rangle = QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

So QFT transforms from the canonical $Z$ basis (computational basis) to the Fourier basis.

**Example** $n = 1$, 1-qubit

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |\tilde{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$|\tilde{j}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i j}|1\rangle)$$

**$N$-qubits System** With 1-qubit, $\{|0\rangle, |1\rangle\}$.
With 2-qubit $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ which is a short-hand writing of $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
With $N$-qubits we have the basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ keeping in mind that it's a short-hand writing, $2^n$ basis states so $2^n$ configuration of bits.
E.g. $|4\rangle = |100\rangle$

For $n = 3$

$$|\tilde{j}\rangle = \frac{1}{\sqrt{2^3}} \sum_{k=0}^{2^3-1} e^{\frac{2\pi i j k}{2^3}} |k\rangle$$

Remembering that

$$|k\rangle = |k_1 k_2 k_3\rangle$$

So the sum must be interpreted as

$$\sum_k = \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \sum_{k_3=0}^{1}$$

In the general case

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle =$$

with $k = k_1 k_2 \ldots k_n$ which are digits of the binary representation, so can be rewritten in decimal representation as $k = \sum_{s=1}^{n} k_s 2^{n-s}$

$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \sum_{s=1}^{n} k_s 2^{-s}} |k_1 \ldots k_n\rangle =$$
$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \prod_{s=1}^{n} e^{\frac{2\pi i j k_s}{2^s}} |k_1 \ldots k_n\rangle =$$

If you isolate the first qubit you get a tensor product because of the $\prod$, and the $sum_k$ decomposes into the sums $\sum_{k_1}\sum_{k_2}\cdots$

$$= \frac{1}{\sqrt{N}}\left(|0\rangle + e^{\frac{2\pi ij}{2^1}}|1\rangle\right)\otimes\left(|0\rangle + e^{\frac{2\pi ij}{2^2}}|1\rangle\right)\otimes\ldots\otimes\left(|0\rangle + e^{\frac{2\pi ij}{2^n}}|1\rangle\right)$$

Each qubit has been transformed into something very similar to an Hadamard gate, except for the exponent of $e$.
So we went from

$$|j\rangle = |j_1\ldots j_n\rangle = |j_1\rangle\otimes\ldots\otimes|j_n\rangle$$

to

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + e^{\frac{2\pi ij}{2^1}}|1\rangle\right)\otimes\ldots\otimes\left(|0\rangle + e^{\frac{2\pi ij}{2^n}}|1\rangle\right)$$

with a 1 to 1 correspondence between bits.

$$|j_s\rangle \mapsto |\tilde{j}_s\rangle = \left(|0\rangle + e^{\frac{2\pi ij}{2^s}}|1\rangle\right)$$

Each gets a bit of information from each configuration, with $s$ affecting the relative phase.

$\frac{1}{\sqrt{N}}e^{\frac{2\pi ij}{2}} \to |10\ldots0\rangle$

$\frac{1}{\sqrt{N}}e^{\frac{2\pi ij}{2^n}} \to |0\ldots01\rangle$

$\frac{1}{\sqrt{N}}e^{\frac{2\pi ij}{2^s}} \to |0\ldots010\ldots0\rangle$

$\frac{1}{\sqrt{N}}\left(e^{\frac{2\pi ij}{2}} + \ldots + e^{\frac{2\pi ij}{2^n}}\right) = \frac{1}{\sqrt{N}}e^{2\pi i(\frac{j}{2}+\ldots+\frac{j}{2^n})} \to |1\ldots1\rangle$

So the the phase applied is qubit dependent

**Example** $n = 3, |j\rangle = |101\rangle$

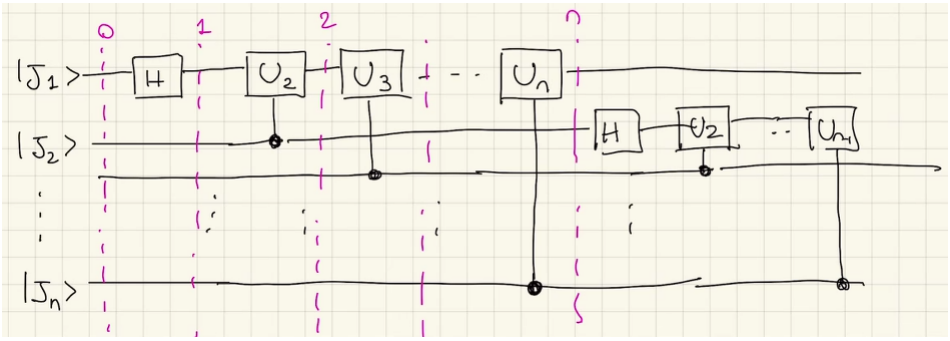
$$|\tilde{5}\rangle = \frac{1}{N}\left(|0\rangle + e^{2\pi i\frac{5}{2}}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i\frac{5}{4}}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i\frac{5}{8}}|1\rangle\right)$$

**Building Blocks for the Circuit**

$H|j_s\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2}j_s}|1\rangle\right)$

Something that depends on the index and does the right rotation: the $U_s$ rotation gate depending on $s$.
$U_s|j_t\rangle \mapsto e^{\frac{2\pi i}{2^s}j_t}|j_t\rangle$
Just applies a phase.

**The Circuit**




1. $|j_1\ldots j_n\rangle$
2. $H|j_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle e^{\frac{2\pi i}{2}j_1}|1\rangle\right)\otimes|j_2\ldots j_n\rangle$
3. Apply the gate only when $j_2$ is 1 (the black dot means that), but that's how $U$ works, it has a 0 on the $|0\rangle$
   $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2}j_1}e^{\frac{2\pi i}{2^2}j_2}|1\rangle\right)\otimes|j_2\ldots j_n\rangle$

4. $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2}j_1} e^{\frac{2\pi i}{2^2}j_2} e^{\frac{2\pi i}{2^3}j_1}|1\rangle\right) \otimes |j_2 \dots j_n\rangle$

   ...

$n$. $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(\frac{j_1}{2}+\frac{j_2}{2^2}+\dots+\frac{j_n}{2^n})}|1\rangle\right) \otimes |j_2 \dots j_n\rangle =$
   And given that $j = \sum_{s=1}^{n} j_s 2^{n-s} = j_1 2^n + j_s^{n-1} + \dots + j_n 2^0$ so we have $\frac{j_1}{2} + \frac{j_2}{2^2} + \dots + \frac{j_n}{2^n} = \frac{1}{2^n}(j_1 2^n + j_s^{n-1} + \dots + j_n 2^0)$ we have that
   $= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i j}{2^n}}|1\rangle\right) \otimes |j_2 \dots j_n\rangle$
   But we end up with the $n$th configuration on the first qubit!

So we implements QFT in the reverse order, applying for example swap gates at the beginning or changing the configuration of the qubits at the end.

**Review**

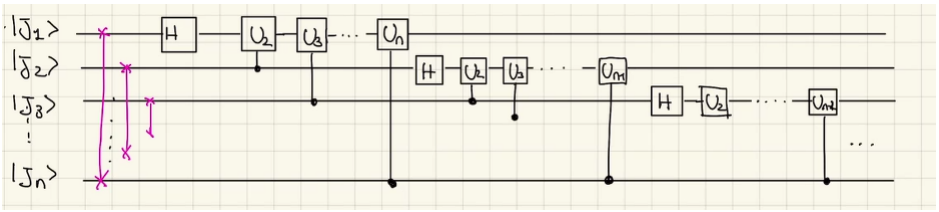
$$|\tilde{j}\rangle = QFT(j) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}}|k\rangle$$

$$|\tilde{j}\rangle = F_N|j\rangle$$

The $j$th column of $F_N$

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & \dots & 1 \\ \vdots & & \\ 1 & & \end{bmatrix} \text{ with the } (j,k) \text{ entry being } e^{\frac{2\pi i j k}{N}}$$

The circuit is

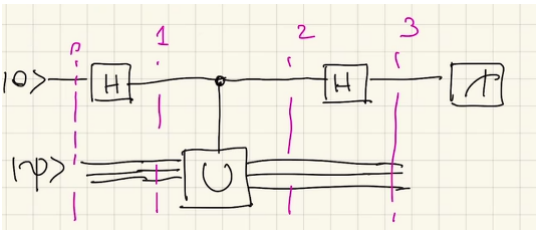



With the swap gates in purple.

**Quantum Phase Estimation** Any unitary matrix is diagonalizable, has an orthonormal basis of eigenvectors and has a set of eigenvalues in the form $e^{i\theta_\psi}$ associated to an eigenstate $|\psi\rangle$

$$U|\psi\rangle = e^{i\theta_\psi}|\psi\rangle$$

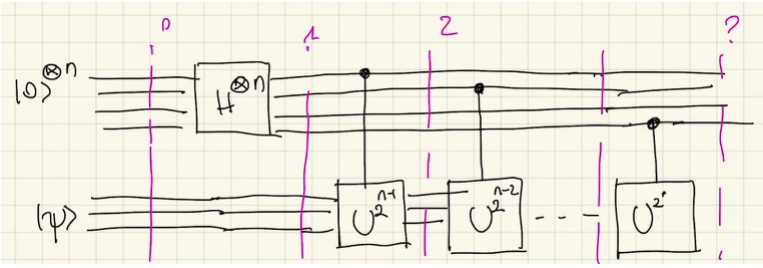
The **QPE problem** is formulated as follows: given that we have the ability of preparing $|\psi\rangle$ and to use $U$, can we extract $\theta_\psi$ which is the angle of the rotation (the **phase**)? Yes, also without QFT. Let's see the intuition on how we could do without QFT.




1. My state is $|0\rangle|\psi\rangle$
2. $|\psi\rangle$ doesn't change and we apply $H$ to $|0\rangle$ which becomes $|+\rangle$
   The state is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle|\psi\rangle$
3. $U$ applies only on the second qubit.
   The state is $\frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}e^{i\theta_\psi}|1\rangle|\psi\rangle$
4. $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, but $H$ applied only on the first qubit.
   The state is $\frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}})|\psi\rangle + \frac{1}{\sqrt{2}}e^{i\theta_\psi}(\frac{|0\rangle-|1\rangle}{\sqrt{2}})|\psi\rangle = \frac{1}{2}[(1+e^{i\theta_\psi})|0\rangle + (1-e^{i\theta_\psi})|1\rangle]|\psi\rangle$

The probability of measuring $|0\rangle$ in the first qubit is the square of the amplitude. So we've encoded the information in the amplitudes, and they are different so I can distinguish them. The drawback is that we perform a complex circuit.

With QFE this is different. $\theta$ in general is $\in R$. The beginning of the QPE circuit is this:



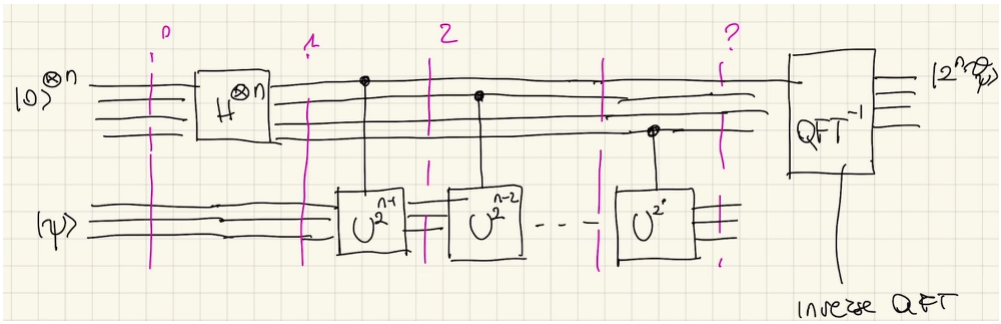

We apply a power of $U$: $U^{2^{n-1}}$ for $n$ bits, all the powers from $2^{n-1}$ to $2^0$.

1. $|0\rangle^{\otimes n}|\psi\rangle$
2. $\left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + |1\rangle)^{\otimes n}|\psi\rangle$
3. We have that
$$U^k|\psi\rangle = \left(e^{i\theta_\psi}\right)^k |\psi\rangle$$
The control bit is entangled, so by applying the $U$ gate the phase kicks back to the control bit.
$$\begin{bmatrix} I & \\ & U \end{bmatrix} \left( \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes |\psi\rangle \right)$$

Final.
$$\left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + e^{i\theta_\psi 2^{n-1}}|1\rangle) \otimes (|0\rangle + e^{i\theta_\psi 2^{n-2}}|1\rangle|) \otimes \ldots \otimes (|0\rangle + e^{i\theta_\psi 2^0}|1\rangle) \otimes |\psi\rangle$$

Now we want to retrieve $\theta_\psi$. The QFT of $|j\rangle$ was
$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i j}{2}}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^n}}|1\rangle\right)$$

These two configurations are very similar, they differ for the exponent. So it's the same of QPE except that $\theta_\psi$ is replace by $\frac{2\pi}{2^n} j$.
The final circuit is composed with the inverse of the QFT, where we need to run the circuit backwards, measuring $|2^n\theta_\psi\rangle$




### 0.5.5 Grover's Algorithm

Searching in an unstructured set of elements, from $O(N)$ to $O(\sqrt{N})$.
We have a list of $N$ objects in a quantum memory and we want to retrieve a target element.
In the classical world, if the list is sorted we have $O(\log N)$ operations with binary search, otherwise in unsorted lists we may do on average $O(\frac{N}{2})$ accesses. In quantum we can do it in $O(\sqrt{N})$.

**Example** Find $x, y, z, w \in N$ with $x, y, z, w \leq 10^6$ such that $x^4 + y^4 + z^4 = w^4$. With a classical brute force approach we have a total number of queries of $\frac{10^{18}}{6}$ (removing permutations). With the quantum algorithm we can lower this number of queries to $\sqrt{N} = 10^9$.

**Grover Iterations** If you have $M$ solutions (targets), you can lower the complexity to $O\left(\sqrt{\frac{N}{M}}\right)$
With $M = 1$, assume the target solution is denoted by $\beta$, the oracle that recognizes the solution is

$$\text{Oracle}(x) = \begin{cases} 0 & x = \beta \\ 1 & x \neq \beta \end{cases}$$

We need to represent in the quantum world this oracle: $U_\beta|x\rangle$. Our database is $\{|0\rangle, \dots, |N-\rangle\}$ with the usual convention that we are representing single qubits (so $\log N$ qubits from all zeros to all ones). This works by changing the phase

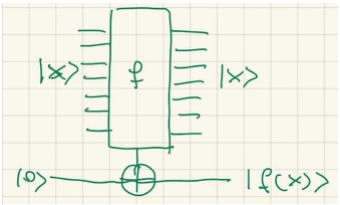
$$U_\beta|x\rangle = \begin{cases} |x\rangle & x \neq \beta \\ -|x\rangle & x = \beta \end{cases}$$

Identity if the state is $\neq \beta$

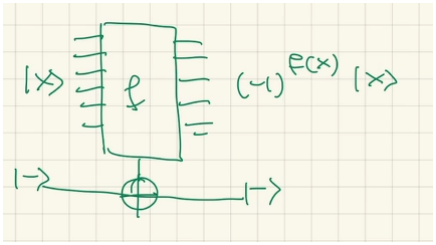
$$U_\beta = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & -1 & \\ & & & & \ddots \end{bmatrix} \text{ with } -1 \text{ in position } (\beta, \beta)$$

$$U_\beta|x\rangle = (-1)^{\text{Oracle}(x)}|x\rangle$$

**Construction of the Grover Oracle** Classical boolean functions can be converted to reversible quantum circuits. $|x\rangle$ enters the circuit that output $|x\rangle$. The circuit is in xor with a $|0\rangle$ that emits $|f(x)\rangle$ such that if $f(x) = 0$ nothing happens, so $|0\rangle \to |0\rangle = |f(x)\rangle$.
If $f(x) = 1$ then $|0\rangle \to |1\rangle = |f(x)\rangle$.




But we don't want to initialize it to $|0\rangle$ but to $|-\rangle$, such that the last register remains $|-\rangle$ and the Oracle outputs $(-1)^{f(x)}|x\rangle$




**Grover Algorithm**

1. Initialize the circuit to uniform superposition (usual Hadamard gates on each qubit), assuming $N = 2^n$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. Perform $t$ times a **Grover Iteration**
3. Measure in the computational basis

The focus is $t$, which we are going to estimate, and proving that the Grover Iterations converge.

$$U_\beta|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0, x\neq\beta}^{N-1} |x\rangle - \frac{1}{\sqrt{N}}|\beta\rangle$$

Measuring will yield one of the $N$ configurations: we changed the phase but not the amplitude. So the Grover Iteration has the goal to amplify the amplitude of the target state in order to make it much bigger than the others.

**Diffuser** The goal is to amplify the amplitude of $\beta$.
Two important states:

$|\psi\rangle$ superposition of all the state

$|\beta\rangle$ the target state

I consider $span\{|\beta\rangle, |\psi\rangle\}$ which is a plane in $R^N$ (dimension 2). They are not orthogonal

$$\langle\beta|\psi\rangle = \frac{1}{\sqrt{N}} \neq 0$$

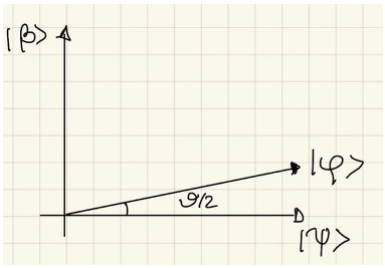
But for very large $N$ they are **almost orthogonal**.
We consider $|\phi\rangle \in span\{|\beta\rangle, |\psi\rangle\}$ such that $\langle\phi|\beta\rangle = 0$: we can take $|\psi\rangle$ and remove the components in directions of $|\beta\rangle$

$$|\phi\rangle = \sqrt{\frac{N}{N-1}}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N}|x\rangle\right) - \frac{1}{\sqrt{N}}|\beta\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\neq\beta}|x\rangle$$

We can also rewrite $|\psi\rangle$

$$|\psi\rangle = \sin\left(\frac{\theta}{2}\right)|\beta\rangle + \cos\left(\frac{\theta}{2}\right)|\phi\rangle = \frac{1}{\sqrt{N}}|\beta\rangle + \sqrt{\frac{N-1}{N}}|\phi\rangle$$

Because $\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \Leftrightarrow \frac{\theta}{2} = \arcsin\frac{1}{\sqrt{N}}$. So the angle between $|\psi\rangle$ and $|\phi\rangle$ is $\frac{\theta}{2}$

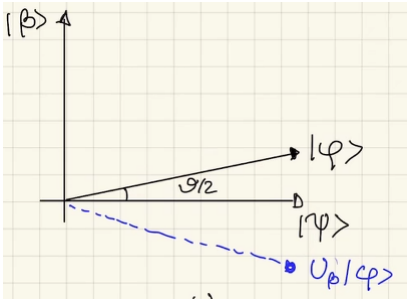



$\psi$ and $\phi$ are inverted

So we start and apply $U_\beta$ to our starting state $|\psi\rangle$

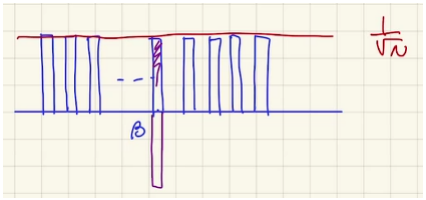
$$U_\beta|\psi\rangle = \cos\frac{\theta}{2}|\phi\rangle - \sin\frac{\theta}{2}|\beta\rangle$$

So it reflects along $|\phi\rangle$: $U_\beta$ is a reflection along the space orthogonal to $|\beta\rangle$.




$\psi$ and $\phi$ are inverted

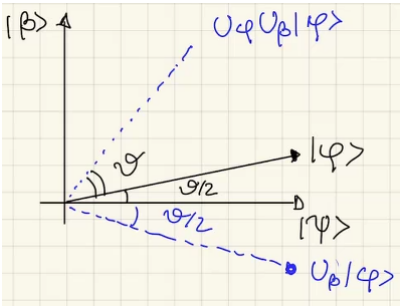
Starting with all equal amplitudes of $\frac{1}{\sqrt{N}}$, the amplitude of $|\beta\rangle$ is inverted!



Then the diffuser step $U_\psi$: reflection around $|\psi\rangle$

$$U_\psi = 2|\psi\rangle\langle\psi| - I$$

We obtain $U_\psi U_\beta|\psi\rangle$ which reflects $U_\beta|\psi\rangle$ around $|\psi\rangle$ with an angle of $\theta$ with $|\psi\rangle$




$\psi$ and $\phi$ are inverted

This reflection is often referred to as inversion around the average. The amplitudes of the configurations $\neq |\beta\rangle$ is lowered to $\frac{N-2}{N\sqrt{N}}$ while the amplitude of $|\beta\rangle$ is amplified.
These reflections are the iterations: start with $|\psi\rangle$, reflect along the $|\phi\rangle$ orthogonal to the target $|\beta\rangle$ and then reflect along $|\psi\rangle$ obtaining $|z\rangle$. Then repeat: reflect $|z\rangle$ along $|\phi\rangle$, reflect along $|\psi\rangle\dots$
At the generic step

$$G = U_\psi U_\beta$$

$$|\psi^{(k)}\rangle = G^k|\psi\rangle = G|\psi^{(k-1)}\rangle$$

Let's denote

$$|z\rangle = U_\beta|\psi^{(k)}\rangle = \sum_{x=0}^{N-1}\alpha_x|x\rangle$$

$$|\psi^{(k+1)}\rangle = U_\psi|z\rangle = (2|\psi\rangle\langle\psi| - I)\left(\sum_{x=0}^{N-1}\alpha_x|x\rangle\right) = 1\sum_{x=0}^{N-1}\alpha_x\langle\psi|x\rangle|\psi\rangle - \sum_{x=0}^{N-1}\alpha_x|x\rangle =$$

$\langle\psi|x\rangle = \frac{1}{\sqrt{N}}$ and $|\psi\rangle$ doesn't depend on $|x\rangle$

$$2\sum_{x=0}^{N-1}\frac{1}{\sqrt{N}}\alpha_x = \frac{2N}{\sqrt{N}}\frac{1}{N}\sum_{x=0}^{N-1}\alpha_x$$

The $M = \frac{1}{N}\sum_{x=0}^{N-1}\alpha_x$ is the average of $z$ so we can rewrite as

$$|\psi^{(k+1)}\rangle = \sum_{x=0}^{N-1}(-\alpha_x + 2M)|x\rangle$$

The first step

$$|\psi^{(1)}\rangle = \left(2M - \frac{1}{\sqrt{N}}\right)\sum_{x\neq\beta}|x\rangle + \left(2M + \frac{1}{\sqrt{N}}\right)|\beta\rangle$$

Can see that the amplitude of $|\beta\rangle$ has increased and the others have decreased by a factor proportional to the mean.

**Number of Iterations** $G = U_\psi U_\beta$ is a rotation: **the composition of two reflectors is a rotation** of an angle $\theta$ where $\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}} \Leftrightarrow \theta = 2\arcsin\frac{1}{\sqrt{N}}$.
$G^k$ has rotated of $\theta^k = (2k+1)\frac{\theta}{2}$ and we want to stop when $(2k+1)\frac{\theta}{2} = \frac{\pi}{2}$, near $|\beta\rangle$ (at 90 degrees).

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

$$k = \left(\frac{\pi}{2} - \frac{\theta}{2}\right)\frac{1}{\theta}$$

But $\frac{\pi}{2}$ is irrational so we want an approximation $(2k+1)\frac{\theta}{2} \simeq \frac{\pi}{2}$

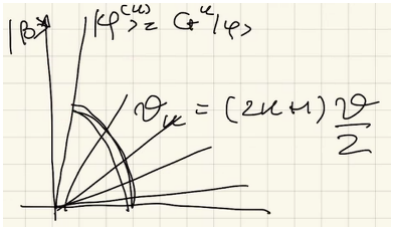
$$k = \lfloor \frac{\pi}{2\theta} - \frac{1}{2} \rfloor$$

For a sufficiently large $N$ we can approximate $\arcsin\left(\frac{\theta}{2}\right) = \frac{\theta}{2} = \frac{1}{\sqrt{N}}$ (from the Taylor expansion of arcsin) getting

$$k \simeq \left(\frac{\pi}{2} - \frac{1}{\sqrt{N}}\right)\frac{\sqrt{N}}{2} = \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$$

So the number of iterations

$$t \simeq \frac{\pi}{4}\sqrt{N}$$



The remaining angle is $\frac{\pi}{2} - (2k+1)\frac{\theta}{2}$

**Theorem** If we perform $k = \lfloor \frac{\pi}{2\theta} - \frac{1}{2} \rfloor \simeq \frac{\pi}{4}\sqrt{N}$ Grover Iterations, the probability of measuring the target state $|\beta\rangle$ is

$$P(\text{Measuring } |\beta\rangle) = 1 - \frac{1}{N}$$

Projecting along $|\beta\rangle$ at time $k$

$$P(\text{Measuring } |\beta\rangle) = |\langle\beta| G^k |\psi\rangle|^2 = \cos^2\left(\frac{\pi}{2} - (2k+1)\frac{\theta}{2}\right) = 1 - \sin^2\left(\frac{\theta}{2}\right) = 1 - \frac{1}{N}$$

**Circuit for the Grover Iteration** $G$ We have $H^{\otimes n}|\psi\rangle = |0\rangle^{\otimes n}$ so $|\psi\rangle = H^{\otimes n}|0\rangle$, also $I = H^{\otimes n}H^{\otimes n}$

$$U_\psi = 2|\psi\rangle\langle\psi| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$$

$$2\begin{bmatrix} 1 & & \\ & & \\ & & 0 \end{bmatrix} - \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix}$$

### 0.5.6 Shor's Algorithm

$N$ composite number: Shor's algorithm can find a factor of $N$ in $O(n^2 \cdot \log n \cdot \log\log n)$ steps, with $n = \lceil \log N \rceil$. Can find factors in NP.
The most efficient classical factoring algorithm (general number field sieve) works in subexponential $O(e^{1.9}n^{1/3(\log n)^{2/3}})$
The decision version of the problem is not NP-complete. All current public key cryptography (RSA, DH, ECC) would be broken if Shor's algorithm could be physically realized.

#### Complexity Classes

**BQP** (Bounded-error Quantum Polynomial Time): class of decision problems that can be solved in polynomial time on a quantum computer, with bounded error probability (at most 1/3 as arbitrary choice, can be 1/2)
The decision version of factoring is in BQP

**BPP** (Bounded-error Polynomial Time): class of decision problems that can be solved in polynomial time using randomized algorithms, if a bounded probability of error is allowed in the solution.
The decision version of factorization is not known to be in BPP.

If indeed factorization $\notin$ BPP, then quantum computer would be the first counterexample to the "strong" Church-Turing Thesis, which states that all reasonable models of computation are polynomially equivalent.

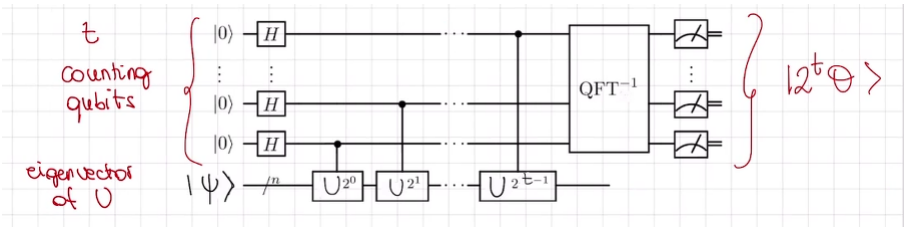
Application of QPE: quantum order-finding. Factorization is solved via a reduction to order-finding.

**Order-Finding Problem** We are given coprime integers $a, N$, meaning $\text{GCD}(a, N) = 1$. The **order**/period of $a$ is the smallest positive integer $r$ such that

$$a^r \bmod N = 1$$

The problem is finding $r$ given $a$ and $N$ with $\text{GCD}(a, N) = 1$.
Also called period because $f(x) = a^x \bmod N$ is periodic with period $r$. Indeed $\forall\ s\ \ f(s + r) = a^{s+r} \bmod N = a^s \bmod N = f(s)$

**Shor's Algorithm** The idea is to use QPE: given $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ with $|\psi\rangle$ eigenvector and $e^{2\pi i\theta}$ corresponding eigenvalues.




The accuracy and the probability of success of QPE depends on the number of counting qubits $t$. Need to define a unitary operator that computes

$$f(x) = a^x \bmod N$$

and whose eigenvalues contain the order $r$, so that we can apply QPE to estimate the eigenvalues and recover $r$.

**Construction of $U_a$** Given $N, n = \lceil \log_2 N \rceil, a$

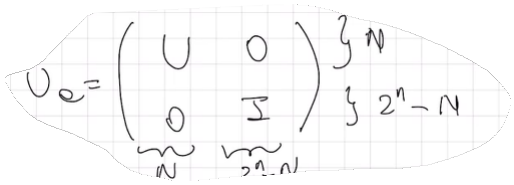
$$U_a|y\rangle = \begin{cases} |a \cdot y \bmod N\rangle & 0 \leq y < N \\ |y\rangle & N \leq y < 2^n \end{cases}$$

Example with $N = 5, a = 3, n = 3$

$$U_a|y\rangle = \begin{cases} |3 \cdot y \bmod 5\rangle & 0 \leq y < 6 \\ |y\rangle & 6 \leq y < 8 \end{cases}$$

Show that $U_a$ is unitary and that it contains the eigenvalue $r$.

**$U_a$ is unitary** It can be described by a block diagonal matrix.




So to prove that $U_a$ is unitary it's enough to prove that $U$ is unitary, so that $U^+U = I$. Given $0 \leq y', y < N$, we need to prove that

$$\langle y'|U^+U|y\rangle = \delta_{yy'} = \begin{cases} 0 & y \neq y' \\ 1 & y = y \end{cases}$$

So we have

$$\langle y'|U^+U|y\rangle =< ay' \bmod N|ay \bmod N\rangle$$

This can happen $\Leftrightarrow$

$$ay' \equiv ay \bmod N$$

Remember that $a$ is coprime with $N$, so we have that $\exists\, a^{-1}$

$$a^{-1}ay' \equiv a^{-1}ay \bmod N$$

$$y' \equiv y \bmod N$$

And $y, y' < N$ so we have an equivalence

$$y' = y$$

So the operator is unitary.

**Eigenvalues of $U_a$** We have

$$U_a^r|y\rangle = U_a^{r-1}|ay \bmod N\rangle = \ldots = |a^r y \bmod N\rangle = |y\rangle$$

Because $r$ is the order. So we have

$$U_a^r|y\rangle = \begin{cases} |y\rangle & 0 \leq y < N \\ |y\rangle & N \leq y < 2^n \end{cases}$$

So $U_a^r = I$ is the identity. This means that the eigenvalues of $U_a$ are the $r$-roots of the unity.

$$\lambda_s = e^{\frac{2\pi i}{r}s} = \omega^s$$

with $0 \leq s < r$ and $e^{\frac{2\pi i}{r}} = \omega$
The phase is $\frac{s}{r}$, and it contains $r$.

**Eigenvectors of $U_a$** $\forall\, 0 \leq s < r$

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{-sk} |a^k \bmod N\rangle$$

is the eigenvector with eigenvalues $\omega^s == e^{\frac{2\pi i}{r}s}$

$$U_a|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{-sk} |a^{k+1} \bmod N\rangle =$$

$$= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \omega^{-s(k-1)} |a^k \bmod N\rangle =$$

$$= \frac{1}{\sqrt{r}} \sum_{k=1}^{r-1} \omega^s \omega^{-sk)} |a^k \bmod N\rangle + \frac{1}{\sqrt{r}} \omega^s \omega^{-sr} |a^r \bmod N\rangle =$$

We have that, in the term corresponding to $k = r$, $\omega^{-sr} = 1$ and $a^r = 1$ by definition of order

$$= \frac{1}{\sqrt{r}} \omega^s \sum_{k=1}^{r-1} \omega^{-sk} |a^k \bmod N\rangle + \frac{1}{\sqrt{r}} \omega^s \omega^{-s0} |a^0 \bmod N\rangle =$$

Observe that the term corresponding to $k = r$ is equal to the term corresponding to $k = 0$.

$$= \frac{1}{\sqrt{r}} \omega^s \sum_{k=0}^{r-1} \omega^{-sk} |a^k \bmod N\rangle = \omega^s |u_s\rangle$$

$$U_a|u_s\rangle = \omega^s |u_s\rangle$$

$$\omega^s = e^{\frac{2\pi i}{r}s}$$

To run QPE we need to prepare the state $|u_s\rangle$, but to prepare it we need $r$ which we do not have.
Instead of preparing $|u_s\rangle$ we prepare a superposition of the eigenvectors.

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{-sk} |a^k \bmod N\rangle =$$

$$= \frac{1}{r} \sum_{s=0}^{r-1} \left( \omega^{-0s} |a^0 \bmod N\rangle + \sum_{k=1}^{r-1} \omega^{-sk} |a^k \bmod B\rangle \right) =$$

$$= \frac{1}{r} \sum_{s=0}^{r-1} |1\rangle + \frac{1}{r} \sum_{k=1}^{r-1} \left( \sum_{s=0}^{r-1} \omega^{-sk} \right) |a^k \bmod N\rangle =$$

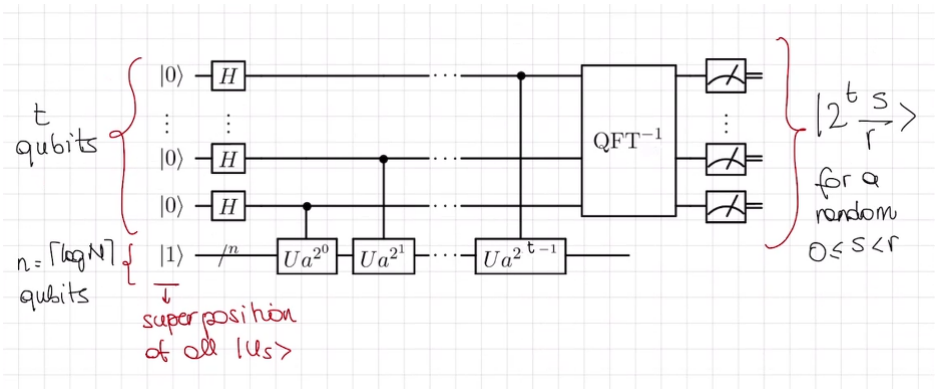
$$= |1\rangle + \frac{1}{r} \sum_{k=1}^{r-1} \left( \frac{1 - (\omega^{-sk})^r}{1 - \omega^{-sk}} \right) |a^k \bmod N\rangle =$$

And $\omega = e^{\frac{2\pi i}{r}}$ so the sum in parenthesis is 0, so the superposition of all the states is just

$$= |1\rangle = |0 \ldots 01\rangle$$

with $n - 1$ zeros and a 1, so $n = \lceil \log N \rceil$ bits.

**Circuit** QPE circuit adapted




$$t = 2n + 1 + \lceil \log\left(2 + \frac{1}{2\epsilon}\right) \rceil$$

With $t$ qubits we will obtain an estimate of $\frac{s}{r}$ accurate to $2n+1$ bits with probability of at least $1-\epsilon$. We need that accuracy to be able to recover $r$ from the phase $\frac{s}{r}$ (with a classical algorithm).
The circuit consists of 4 steps

1. Apply $t$ Hadamard gates to put the first counting qubits register in equal superposition.

$$|0\rangle^{\otimes n}|1\rangle \mapsto \frac{1}{\sqrt{2^t}} \sum_{j=0}^{t-1} |j\rangle|1\rangle$$

2. Apply the sequence of controlled $U_a^{2^j}$ gates with control on the $j$th qubit.

$$\frac{1}{\sqrt{r \cdot 2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \omega^{sj} |j\rangle|u_s\rangle$$

3. Apply the inverse Quantum Fourier Transform on the first register and we get a superposition of eigenvectors $|u_r\rangle$ entangled with estimates of their corresponding eigenvalues

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |2^t \frac{s}{r}\rangle|u_s\rangle$$

   So a superposition of estimates instead of a single estimate like in QPE

4. Measure the first register, and since there is a superposition we have each estimate with equal probability. The uniform superposition collapses to one of the $r$ eigenvectors $|u_s\rangle$ and QPE returns an estimate of the phase $\frac{s}{r}$ for a random (unknown) $s$ with $0 \leq s < r$

**Implementing $U_a$ Efficiently** Using fast exponentiation: square and multiply (quadrature successive).
The idea is that

$$U_a^{2^j}|y\rangle = |a^{2^j} y \bmod N\rangle =$$

But we take the modulo immediately

$$= |(a^{2^j} \bmod N) y \bmod N\rangle$$

So we precompute all values

$$a \bmod N, a^2 \bmod N, a^4 \bmod N, \ldots, a^{2^j} \bmod N, \ldots, a^{2^{t-1}} \bmod N$$

These are all $n$ bit numbers, and we can compute all of them with $t-1$ operations, $O(n^2)$ or $O(n \log n \log\log n)$ with fast multiplication. $t$ is $O(n)$ therefore the cost is $O(n^2 \log n \log\log n)$ with fast multiplication.

$$U_a^{2^j}|y\rangle = |(a^{2^j} \bmod N) y \bmod N\rangle$$

**Recovering $r$ from the Phase $\frac{r}{s}$** This is classical computation, doesn't require quantum computation and is performed on a classical computer applying the **Continued Fractions Algorithm** CFA.

On the first register we measure an integer $x = 2^t \frac{s}{r}$ for unknown $r$ and $s$.
So $\frac{x}{2^t} = \phi \simeq \frac{s}{r}$ is an estimate, we only know $2n+1$ bits of $\phi$.

**Easy case**
Suppose that $r$ divides $2^t$, then we know exactly $\phi$ because $\frac{x}{2^t} = \frac{s}{r}$
The fraction is known because we know $x$ and $t$, and to get $r$ we reduce the fraction $\frac{x}{2^t}$ to the lowest terms (to an irreducible fraction). Then we test the denominator $r'$ if it's $r$: we compute $a^{r'} \bmod N$ and if its 1 we're done.
This works if $r, s$ are coprime.

**General case**
We don't know $\phi$ exactly but just $2n+1$ bits of $\phi$. We apply CFA to compute the nearest fraction to $\phi$ with denominator $\leq N$. We take this denominator as tentative order, as $r'$.
This produces the fraction $\frac{s'}{r'}$ with $s', r'$ without common factors, and we check whether $a^{r'} \bmod N = 1$. If so, we're done, else we run again. Even in this case, the procedure requires $r, s$ coprime.

**Quantum Order Finding**

1. Initial state is $|0\rangle|1\rangle$ ($t$ and $n$ qubits)
2. Create a superposition on the first register
$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$$
3. Apply the sequence of controlled $U_a^{2^j}$ gates
$$\frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{\frac{2\pi i s j}{r}} |j\rangle|u_s\rangle$$
4. Apply inverse Fourier transform to the first register
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |2^t \frac{s}{r}\rangle|u_s\rangle$$
5. Measure the first register, estimating $\psi$ of $\frac{s}{r}$
6. Apply CFA obtaining $r$

The overall cost for order-finding with fast multiplication is $O(n^2 \log n \log\log n)$, while the best classical algorithm is $O(e^{\sqrt{n \log n}})$, but of course the quantum algorithm can fail because QPE can produce a bad estimate for $\frac{s}{r}$ with probability at most $\epsilon$ thanks to our choice of $t$.
If $r, s$ have a common factor, the number $r$ returned but the CFA is a factor of $r$, not $r$ itself. So $r, s$ should be co-prime.

**Factorization $\leq$ Order-Finding** Reduction from factoring to order-finding.
$N > 1$ composite, odd and not a prime nor a prime power (we can already test these cases and exclude them in the beginning). So $N$ is a product of at least two primes.
We take $a < N$ and coprime with $N$ ($\text{GCD}(a, N) = 1$). If it's not coprime, we've found a factor of $N$. Suppose that is coprime. We compute the order $r = \text{Order}(a)$. So we know that $a^r \bmod N = 1$, which can be written as

$$(a^r - 1) \bmod N = 0$$

Suppose that $r$ is even, we can write

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \bmod N = 0$$

$1 < a < N$ so the possible cases are:

The first factor $a^{\frac{r}{2}} - 1 \bmod N = 0$ But this means

$$a^{\frac{r}{2}} \bmod N = 1$$

which is impossible per definition of order.

We could have the second factor $a^{\frac{r}{2}} + 1 \bmod N = 0$ means that

$$a^{\frac{r}{2}} \bmod N = -1$$

This can happen, the reduction fails and we need to start over with a different $a$

Both terms are $\neq 0 \bmod N$, this means that $N$ divides $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$ and any factor of $N$ is a factor of $(a^{\frac{r}{2}} - 1)$ or $(a^{\frac{r}{2}} + 1)$ or both. This factor cannot be $N$ (excluded before, non zero modulo $N$).
Using Euclid's algorithm we compute $\text{GCD}(a^{\frac{r}{2}} - 1, N)$ and $\text{GCD}(a^{\frac{r}{2}} + 1, N)$ and find a factor of $N$.

**Shor's Algorithm** Input: a positive integer $N$ with $n = \lceil \log_2 N \rceil$ bits.
Output: a factor $p$ of $N$

1. If $N$ is even, output 2 and stop
2. Use a polynomial time algorithm to determine if $_N$ is a prime or a power of a prime. If this is the case, declare it and stop.
3. Randomly choose an integer $a$ such that $1 < a < N$ and run Euclid's algorithm to determine $GCD(a, N)$. If it's $> 1$, return it and stop.
4. If $a$ and $N$ are coprime, use a Quantum Circuit to find the order $r$ of $a \bmod N$
5. If $r$ is even and $a^{r/2} \bmod N \neq -1$ compute $\text{GCD}(a^{\frac{r}{2}} - 1, N)$ and $\text{GCD}(a^{\frac{r}{2}} + 1, N)$ and return at least one non trivial factor of $N$.
   Otherwise

**Observations** The algorithm returns with high probability a non trivial factor of any composite $N$.
All steps can be performed efficiently on a classical computer, except (as far as we know) the order-finding step (step 4). By repeating the procedure, we may find a complete prime factorization of $N$.

**Complexity** Polynomial in $n = \lceil \log_2 N \rceil$. It take $O(n^2 \log n \log \log n)$ quantum gates using fast multiplication and the square-and-multiply algorithm.

**Success Probability** A single run only returns a factor of $N$ with a certain probability.

The order-finding step could return an odd $r$

The order-finding step could return $r \mid a^{r/2} \bmod N \equiv -1$

The reduction to the order-finding problem doesn't work if $r \equiv 1 \bmod 2$ or $a^{r/2} \bmod N \equiv -1$

**Theorem** Let $N = \prod_{j=1}^{k} p_j^{n_j}$ be the factorization of $N$, with $p_i \neq p_j$ for $i \neq j$. If $a$ is a random element in $Z_N^*$ (i.e. $0 < a < N$ and coprime with $N$), and $r = order(a)$ then

$$P\left(r \equiv 0 \bmod 2 \wedge a^{r/2} \not\equiv -1 \bmod N\right) \geq 1 - \frac{1}{2^k}$$

The algorithm only needs to be repeated a constant number of times to successfully factor $N$ with a high probability of success. The expected number of iterations needed to find a factor doesn't grow with $N$. Shor's algorithm can factor in a number of operations polynomial in the dimension of $N$.
**Exponential speed-up** compared to the best classical algorithm.