ICGM

Institut Charles Gerhardt Montpellier

CHEMISTRY: MOLECULES TO MATERIALS

CNRS · Université de Montpellier · ENSCM Chimie Montpellier · MUSE Pôle Chimie · Institut Carnot Chimie Balard Cirimat

Chimie Physique Théorique
et Modélisation

CHEMISTRY: MOLECULES TO MATERIALS

Introduction to Quantum Computation

Part 1

Bruno Senjean
ICGM, Université de Montpellier, CNRS

Please connect to `http://www.quizzoodle.com/session/join/`

December 12, 2022

Table of contents

History

Classical Computation
- Classical circuit
- Toward the second quantum revolution

Quantum Mechanics

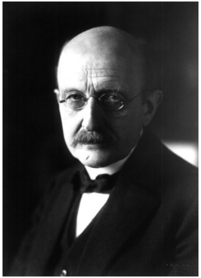
Quantum Computation
- Quantum bit (Qubit)
- Quantum circuit
- Quantum Gates
- Examples

Classical versus Quantum
- Reversibility
- Universality
- No-cloning theorem

History

1900 — Present

Max Planck



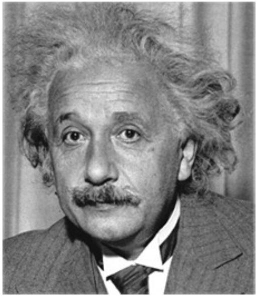
Ultraviolet catastrophe

Planck assumed that electromagnetic radiation can be emitted or absorbed only in discrete packets, called quanta, of energy

$$E = h\nu$$

1905 — Present

Albert Einstein



Photoelectric effect, Interaction light-matter:

a beam of light is not a wave propagating through space,
but a swarm of discrete energy packets, known as photons

1920 — Present

Werner Heisenberg

Max Born

Erwin Schrödinger

Matrix mechanics and Schrödinger wave formulation of quantum states, wavefunctions...

Disruptive mathematical formalism, questioning:

classical waves, corpuscles, trajectories, locality and determinism

1924 Present

Max Born

"Quantum Mechanics" is used for the first time

1932 — Present

John von Neumann

Equivalence between the wave formulation and the matrix mechanics. These equivalent theory will be referred to Quantum Mechanics

1935 — Present

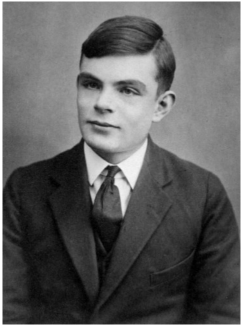
A. Einstein B. Podolski N. Rosen

EPR paper:

Quantum Mechanics is incomplete. It lacks some essential "element of reality".
We are just missing some hidden variable, Nature properties should be deterministic.

1936 — Present

Alan Turing

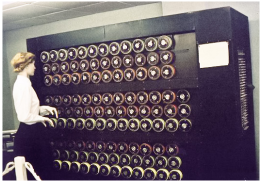


Turing Machine

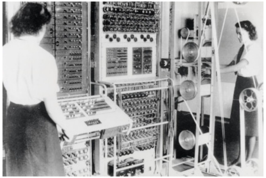
Mathematical model of computation describing an abstract machine capable of implementing any computer algorithm.

1943 — Present

Bombe



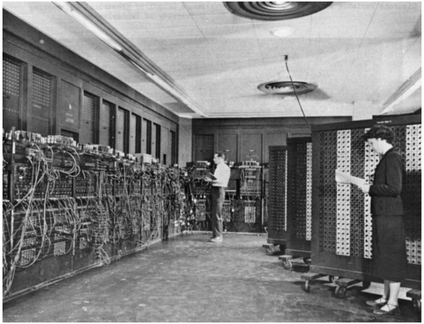
Colossus



Computers used in the Second World War to decode Enigma, just in time for the Normandy landings

1945 — Present

ENIAC (Pennsylvanie)



First programmable, electronic,
general-purpose digital computer,
Turing-complete (computationally universal)
able to simulate any Turing machine.

30 tons, 72 m^2

1947 — Present

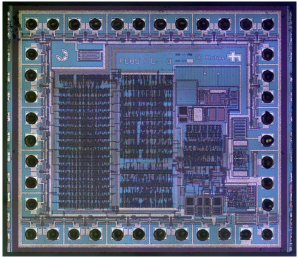
J. Bardeen, W. Brattain, W. Shockley

First working transistor.

A transistor is a semiconductor device
used to amplify or switch electrical signals and power.
The transistor is one of the
basic building blocks of modern electronics.

The first quantum revolution begins

1960 — Present



Integrated circuits

Orders of magnitude smaller, faster, and less expensive

1964 Present

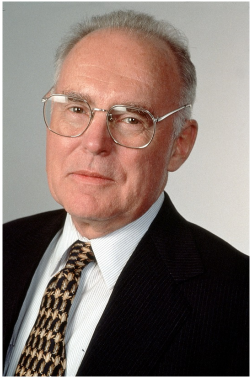
John Stewart Bell

Bell's inequality

Experimental test to check whether or not the picture of the world which EPR were hoping to force a return is valid or not.

1965 — Present

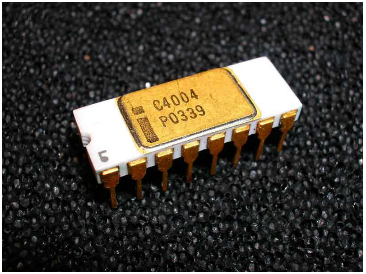
Gordon Earle Moore



Moore's law

Based on the empirical observation that
the number of transistors in a dense integrated circuit
doubles about every two years

1970 Present



Microprocessors

Computer processor where the data processing logic and control is included on a single integrated circuit

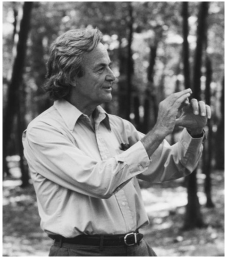
1981 — Present

Paul A. Benioff

First Conference on the Physics of Computation (MIT)

A computer can operate under the laws of quantum mechanics
by describing a Schrödinger equation description of Turing machines.
(foundation for future work on quantum computing)

Richard Feynman



It appears impossible to efficiently simulate an evolution
of a quantum system on a classical computer.
Proposed a basic model for a quantum computer.
(Quantum simulation, advantage over classical computing?)

1982 — Present

William Wootters

Wojciech H. Zurek

No-cloning theorem

impossible to create an independent and identical copy of an arbitrary unknown quantum state

1982 Present

Alain Aspect

First quantum mechanics experiment
to demonstrate the violation of Bell's inequalities

1985 — Present

David Elieser Deutsch

First **universal** quantum computer
(Quantum Turing-Machine)

Universal Turing machine can simulate any other Turing machine efficiently (Church-Turing thesis)

Universal quantum computer can simulate any other quantum computer with at most a **polynomial slowdown**.

(**quantum gates**, similar traditional digital computing binary logic gates)

1988 Present

Yoshihisa Yamamoto

Proposal for first experimental realization of a quantum computer with two-qubit gates using photons and atoms.

1992 — Present

David Elieser Deutsch

Richard Jozsa

Deutsch-Jozsa quantum algorithm.

Although of little current practical use,
it is one of the first examples of a quantum algorithm
that is **exponentially faster**
than any possible deterministic classical algorithm.

1993 Present

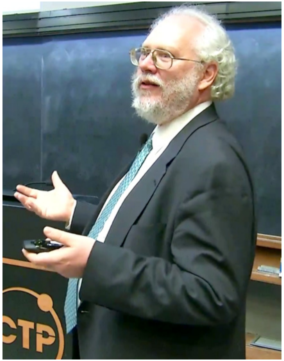
Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels

Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters
Phys. Rev. Lett. **70**, 1895 – Published 29 March 1993

Only the information about the quantum state and not the state itself
(no matter or energy) passes from Alice to Bob.

1994 — Present

Peter Shor



Shor's quantum algorithm.

Finding the prime factors of an integer.

Almost exponentially faster than associated classical algorithms

Quantum cryptography

1995 Present

Ignacio Cirac

Peter Zoller

Proposed an experimental realization of the controlled-NOT gate with cold trapped ions

Christopher Monroe

David J. Wineland

experimentally realize the first quantum logic gate (controlled-NOT gate) with trapped ions

1995 — Present

Alexei Kitaev

Phase estimation algorithm

Estimates the phase (or eigenvalue) of an eigenvector of a unitary operator

1996 Present

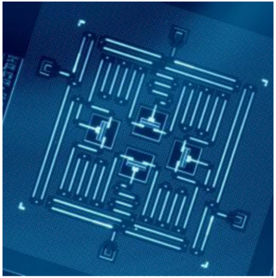
Lov Grover

Quantum search algorithm

Quadratic speed-up over the best analog classical algorithm

1999 Present

Four superconducting transmon qubits



Yasunobu Nakamura and Jaw-Shen Tsai

demonstrate that a superconducting circuit can be used as a qubit

2014 Present

A variational eigenvalue solver on a photonic quantum processor

Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik & Jeremy L. O'Brien

Nature Communications **5**, Article number: 4213 (2014) | Cite this article

Development of an hybrid quantum/classical algorithm
Reduce circuit depth at the expense of measurement and classical optimization

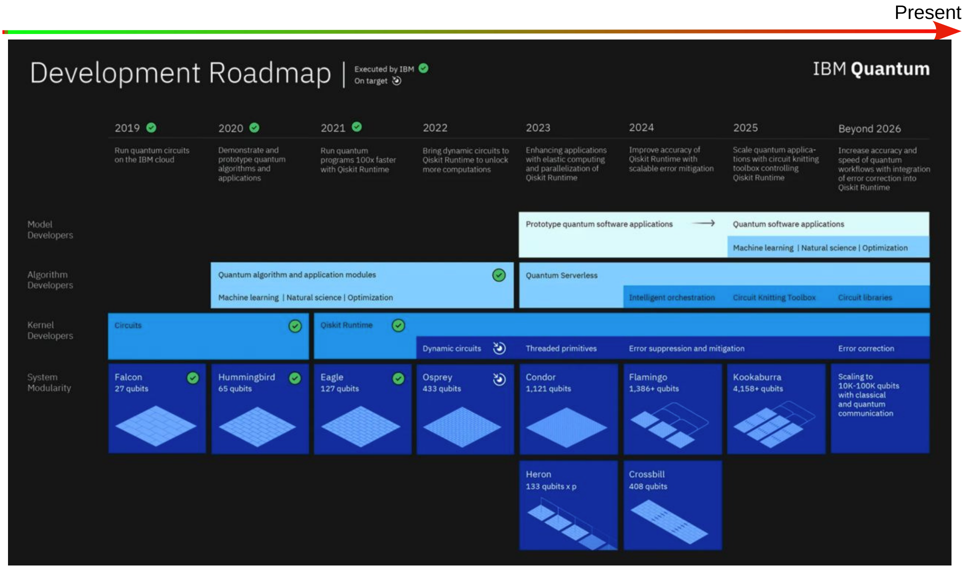
2019 Present

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, ... John M. Martinis + Show authors

Nature **574**, 505–510 (2019) | Cite this article

First experimental demonstration of quantum "**supremacy**" (mitigated by several other authors) for a very specific task.


Present
Development Roadmap
Executed by IBM
On target
IBM Quantum
2019
2020
2021
2022
2023
2024
2025
Beyond 2026
Run quantum circuits on the IBM cloud
Demonstrate and prototype quantum algorithms and applications
Run quantum programs 100x faster with Qiskit Runtime
Bring dynamic circuits to Qiskit Runtime to unlock more computations
Enhancing applications with elastic computing and parallelization of Qiskit Runtime
Improve accuracy of Qiskit Runtime with scalable error mitigation
Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime
Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers
Algorithm Developers
Kernel Developers
System Modularity
Prototype quantum software applications
Quantum software applications
Machine learning | Natural science | Optimization
Quantum algorithm and application modules
Machine learning | Natural science | Optimization
Quantum Serverless
Intelligent orchestration
Circuit Knitting Toolbox
Circuit libraries
Circuits
Qiskit Runtime
Dynamic circuits
Threaded primitives
Error suppression and mitigation
Error correction
Falcon
27 qubits
Hummingbird
65 qubits
Eagle
127 qubits
Osprey
433 qubits
Condor
1,121 qubits
Flamingo
1,386+ qubits
Kookaburra
4,158+ qubits
Scaling to 10K-100K qubits with classical and quantum communication
Heron
133 qubits x p
Crossbill
408 qubits

Classical Computation

Classical circuit

Classical bits

The basic component of classical information is the *classical bit* (binary digit) which can take the value 1 or 0, experimentally corresponding to the state of a transistor, a voltage, or a flux of photons in an optic fiber.

Although the electronic components which create, store and manipulate classical bits rely on quantum mechanics (*first quantum revolution*), the classical bit states are described by classical mechanics, essentially because they involve a huge number of particles.

Classical bits

The basic component of classical information is the *classical bit* (binary digit) which can take the value 1 or 0, experimentally corresponding to the state of a transistor, a voltage, or a flux of photons in an optic fiber.

Although the electronic components which create, store and manipulate classical bits rely on quantum mechanics (*first quantum revolution*), the classical bit states are described by classical mechanics, essentially because they involve a huge number of particles.

Information is stored as a succession of bits, encoding integer numbers and real numbers. For N bits:

$$n = \sum_{i=0}^{N-1} a_i 2^i \xrightarrow{\text{digitization}} a_{N-1}a_{N-2}\ldots a_1 a_0.$$

With N bits, one can encode 2^N integer numbers (*one* at a time).

Classical bits: examples

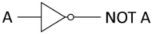
QUIZZ

Classical logical gates

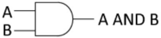
A logic gate is an idealized or physical device implementing a *Boolean function*, a logical operation performed on one or more binary inputs that produces a single binary output.

Classical logical gates

A logic gate is an idealized or physical device implementing a *Boolean function*, a logical operation performed on one or more binary inputs that produces a single binary output.

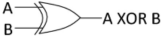


A	NOT A
0	1
1	0

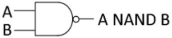


A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

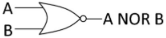
A	B	A OR B
0	0	0
0	1	1
1	0	1
1	1	1



A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0



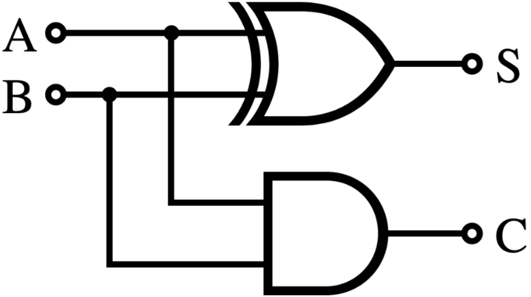
A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0



A	B	A NOR B
0	0	1
0	1	0
1	0	0
1	1	0

Classical circuit: model of classical computation

Example: the half adder circuit



A	B	S A + B	C Retenu
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

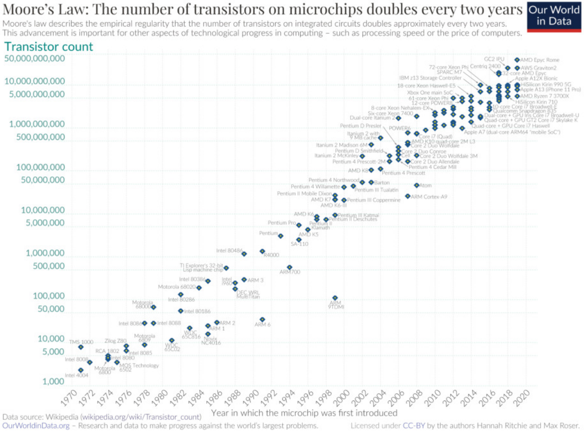
Toward Second Quantum Revolution

Moore's law

The calculation power of a computer is related to the number of transistor in the processor, which has been observed to double about every two years.

Moore's law

The calculation power of a computer is related to the number of transistor in the processor, which has been observed to double about every two years.



The end of Moore's law ?

Transistors are reaching a size where *quantum effects* are *not negligible* anymore ! $\sim$ 2 nm

The end of Moore's law ?

Transistors are reaching a size where *quantum effects* are *not negligible* anymore ! ~ 2 nm

There might be different solutions: 3D stacking, new emergent technologies (post-silicon era), ...

The end of Moore's law ?

Transistors are reaching a size where *quantum effects* are *not negligible* anymore ! ~ 2 nm

There might be different solutions: 3D stacking, new emergent technologies (post-silicon era), ...

But why not a change of paradigm ? Exploit the quantum effects instead of dealing with them !

Toward Quantum Computing

QUIZZ

Quantum Mechanics

Postulates

Postulate 1a: Quantum state of a system

Associated to any isolated physical system is a complex vector space with inner product (Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Postulate 1a: Quantum state of a system

Associated to any isolated physical system is a complex vector space with inner product (Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Consider an orthonormal basis $\{|\alpha_i\rangle\}$ for a d-dimensional state space. An arbitrary state vector in the state space can be written as:

$$|\psi\rangle = \sum_{i=1}^{d} a_i |\alpha_i\rangle$$

We say that $|\psi\rangle$ is a *superposition* of the states $|\alpha_i\rangle$ with associated *amplitude* a_i.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle \psi | \psi \rangle = 1 \longleftrightarrow \sum_{i=1}^{d} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta} |\psi\rangle$ is also normalized.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle\psi|\psi\rangle = 1 \longleftrightarrow \sum_{i=1}^{d} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta}|\psi\rangle$ is also normalized.

States that differ by this *global phase factor* are said to be *equivalent*.

States that differ by a *relative phase* are distinct.

Postulate 1a: Quantum state of a system

For a physical system, the associated state vector is **normalized**:

$$\langle\psi|\psi\rangle = 1 \longleftrightarrow \sum_{i=1}^{d} |a_i|^2 = 1$$

The unit norm constraint *does not* completely determine $|\psi\rangle$, as any state $e^{i\theta}|\psi\rangle$ is also normalized.

States that differ by this *global phase factor* are said to be *equivalent*.

States that differ by a *relative phase* are distinct.

What about a composite system made up of two (or more) distinct physical systems ?

Postulate 1b: Quantum state of composite systems

The state space of a composite physical system is the **tensor product** of the state spaces of the component physical systems, $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Postulate 1b: Quantum state of composite systems

The state space of a composite physical system is the **tensor product** of the state spaces of the component physical systems, $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

For composite systems A and B, prepared in the state $|\psi_A\rangle$ and $|\psi_B\rangle$, respectively, then the joint state of the total system is

$$|\psi\rangle \quad = \quad |\psi_A\rangle \otimes |\psi_B\rangle \equiv |\psi_A\rangle\,|\psi_B\rangle \equiv |\psi_A\psi_B\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_d \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_1 b_d \\ a_2 b_1 \\ \vdots \\ a_d b_d \end{pmatrix}$$

QUIZZ

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |\alpha_i\rangle \otimes |\beta_j\rangle$.

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |\alpha_i\rangle \otimes |\beta_j\rangle$.

Examples: consider $|\psi_{A,1}\rangle$ and $|\psi_{A,2}\rangle$ ($|\psi_{B,1}\rangle$ and $|\psi_{B,2}\rangle$) two states of system A (B), then

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|\psi_{A,1}\psi_{B,2}\rangle + |\psi_{A,2}\psi_{B,1}\rangle \Big)$$

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |\alpha_i\rangle \otimes |\beta_j\rangle$.

Examples: consider $|\psi_{A,1}\rangle$ and $|\psi_{A,2}\rangle$ ($|\psi_{B,1}\rangle$ and $|\psi_{B,2}\rangle$) two states of system A (B), then

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|\psi_{A,1}\psi_{B,2}\rangle + |\psi_{A,2}\psi_{B,1}\rangle \Big)$$

is **entangled** and

$$|\psi\rangle = \frac{1}{2}\Big(|\psi_{A,1}\psi_{B,1}\rangle + |\psi_{A,1}\psi_{B,2}\rangle + |\psi_{A,2}\psi_{B,1}\rangle + |\psi_{A,2}\psi_{B,2}\rangle \Big)$$

Postulate 1b: Quantum state of composite systems

Any state of $\mathcal{H}$ can be decomposed in the basis $\{|\mu_{ij}\rangle\}$ formed by the tensor product of the basis of $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e. $|\mu_{ij}\rangle = |\alpha_i\rangle \otimes |\beta_j\rangle$.

Examples: consider $|\psi_{A,1}\rangle$ and $|\psi_{A,2}\rangle$ ($|\psi_{B,1}\rangle$ and $|\psi_{B,2}\rangle$) two states of system A (B), then

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|\psi_{A,1}\psi_{B,2}\rangle + |\psi_{A,2}\psi_{B,1}\rangle \Big)$$

is **entangled** and

$$|\psi\rangle = \frac{1}{2}\Big(|\psi_{A,1}\psi_{B,1}\rangle + |\psi_{A,1}\psi_{B,2}\rangle + |\psi_{A,2}\psi_{B,1}\rangle + |\psi_{A,2}\psi_{B,2}\rangle \Big) = \frac{1}{2}\Big(|\psi_{A,1}\rangle + |\psi_{A,2}\rangle \Big) \otimes \Big(|\psi_{B,1}\rangle + |\psi_{B,2}\rangle \Big)$$

is **not**.

Entangled states are interesting because they exhibit *correlations* that have *no classical analog*.

Postulate 2: Measurement of physical observable

Every measurable physical quantity $\mathcal{M}$ is described by a Hermitian operator $\hat{\mathcal{M}}$ acting in the state space $\mathcal{H}$. This operator is an observable, meaning that its eigenvectors form a basis for $\mathcal{H}$. The result of measuring a physical quantity $\mathcal{M}$ must be one of the eigenvalues of the corresponding observable $\hat{\mathcal{M}}$.

Postulate 2: Measurement of physical observable

Every measurable physical quantity $\mathcal{M}$ is described by a Hermitian operator $\hat{\mathcal{M}}$ acting in the state space $\mathcal{H}$. This operator is an observable, meaning that its eigenvectors form a basis for $\mathcal{H}$. The result of measuring a physical quantity $\mathcal{M}$ must be one of the eigenvalues of the corresponding observable $\hat{\mathcal{M}}$.

Consider the *spectral decomposition* of $\hat{\mathcal{M}}$:

$$\hat{\mathcal{M}} = \sum_m m\hat{P}_m = \sum_m m \left|m\right\rangle \left\langle m\right|$$

where $\hat{P}_m$ is the *projector* onto the eigenspace of $\hat{\mathcal{M}}$ with eigenvalue m.

The possible outcomes of the measurement are the eigenvalues m of the observable.

Postulate 2: Projective measurement on state $|\psi\rangle$

Consider a state $|\psi\rangle \in \mathcal{H}$, which can always be written in the eigenbasis of $\hat{\mathcal{M}}$:

$$|\psi\rangle = \sum_m \psi_m |m\rangle$$

The *probability* of getting the eigenvalue m upon measuring $|\psi\rangle$ is given by

$$p_\psi(m) = \langle\psi| \hat{P}_m |\psi\rangle = |\langle\psi|m\rangle|^2 = |\psi_m|^2$$

Given that outcome m occurred, $|\psi\rangle$ *collapses* immediately to

$$|\psi\rangle \longrightarrow \frac{\hat{P}_m |\psi\rangle}{\sqrt{p_\psi(m)}} = |m\rangle$$

Postulate 2: Projective measurement, expectation value

One can easily calculate average values for projective measurements,

$$\begin{aligned}
\mathbf{E}_\psi(\hat{\mathcal{M}}) &= \sum_m p_\psi(m) \\
&= \sum_m m \langle\psi| \hat{P}_m |\psi\rangle \\
&= \langle\psi| \left(\sum_m \hat{P}_m\right) |\psi\rangle \\
&= \langle\psi| \hat{\mathcal{M}} |\psi\rangle \equiv \langle\hat{\mathcal{M}}\rangle_\psi
\end{aligned}$$

It follows a formula for the standard deviation

$$\Delta_\psi \hat{\mathcal{M}} = \sqrt{\langle\hat{\mathcal{M}}^2\rangle_\psi - \langle\hat{\mathcal{M}}\rangle_\psi^2}$$

which is a measure of the typical spread of the observed values upon measurement of $\hat{\mathcal{M}}$.

Postulate 3: Time evolution of a system

The time evolution of the state vector $|\psi(t)\rangle$ *is governed by the Schrödinger equation, where* $H(t)$ *is the (time-dependent) Hamiltonian (observable associated with the total energy of the system),*

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

Postulate 3: Time evolution of a system

The time evolution of the state vector $|\psi(t)\rangle$ is governed by the Schrödinger equation, where $H(t)$ is the (time-dependent) Hamiltonian (observable associated with the total energy of the system),

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

or, equivalently:

The time evolution of a closed system is described by a unitary transformation on the initial state,

$$|\psi(t)\rangle = U(t;t_0)|\psi(t_0)\rangle$$

Operation are *unitary* to preserve the norm of the quantum state in time.

Quantum Computation

Quantum Bit or Qubit

Quantum bit: a mathematical object

A *quantum bit (qubit)* is the basic component of quantum computers and is the simplest quantum system: a *two-level system*.

Quantum bit: a mathematical object

A *quantum bit (qubit)* is the basic component of quantum computers and is the simplest quantum system: a *two-level system*.

Any state of the state space will be decomposed in the *computational basis* made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

Quantum bit: a mathematical object

A *quantum bit (qubit)* is the basic component of quantum computers and is the simplest quantum system: a *two-level system*.

Any state of the state space will be decomposed in the *computational basis* made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

In contrast with a classical bit, the state can be something else than $|0\rangle$ and $|1\rangle$, it can be a ***superposition*** of $|0\rangle$ and $|1\rangle$ (also called *quantum parallelism*).

Quantum bit: a mathematical object

A *quantum bit (qubit)* is the basic component of quantum computers and is the simplest quantum system: a *two-level system*.

Any state of the state space will be decomposed in the *computational basis* made out of two vectors denoted $|0\rangle$ and $|1\rangle$ as follows

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$$

with $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$.

In contrast with a classical bit, the state can be something else than $|0\rangle$ and $|1\rangle$, it can be a ***superposition*** of $|0\rangle$ and $|1\rangle$ (also called *quantum parallelism*).

A qubit follows the law of quantum mechanics. It *cannot be examined* to determine its quantum state, but its measurement outcome will be $|0\rangle$ with probability $|\psi_0|^2$ or $|1\rangle$ with probability $|\psi_1|^2$.

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \, \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \, \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

4-qubit: $|\psi\rangle = \psi_0 |0000\rangle + \psi_1 |0001\rangle + \psi_2 |0010\rangle + \psi_3 |0011\rangle \, \psi_4 |0100\rangle + \psi_5 |0101\rangle + \psi_8 |0110\rangle + \psi_7 |0111\rangle$
$+\psi_8 |1000\rangle + \psi_9 |1001\rangle + \psi_{10} |1010\rangle + \psi_{11} |1011\rangle \, \psi_{12} |1100\rangle + \psi_{13} |1101\rangle + \psi_{14} |1110\rangle + \psi_{15} |1111\rangle$

Quantum corollary to Moore's law: Quantum registers

1-qubit: $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$

2-qubit: $|\psi\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$

3-qubit: $|\psi\rangle = \psi_0 |000\rangle + \psi_1 |001\rangle + \psi_2 |010\rangle + \psi_3 |011\rangle \psi_4 |100\rangle + \psi_5 |101\rangle + \psi_8 |110\rangle + \psi_7 |111\rangle$

4-qubit: $|\psi\rangle = \psi_0 |0000\rangle + \psi_1 |0001\rangle + \psi_2 |0010\rangle + \psi_3 |0011\rangle \psi_4 |0100\rangle + \psi_5 |0101\rangle + \psi_8 |0110\rangle + \psi_7 |0111\rangle$
$+\psi_8 |1000\rangle + \psi_9 |1001\rangle + \psi_{10} |1010\rangle + \psi_{11} |1011\rangle \psi_{12} |1100\rangle + \psi_{13} |1101\rangle + \psi_{14} |1110\rangle + \psi_{15} |1111\rangle$

The number of binary strings that are encoded on the qubit register *doubles for every additional qubit*.

That's the **Quantum corollary** to Moore's law

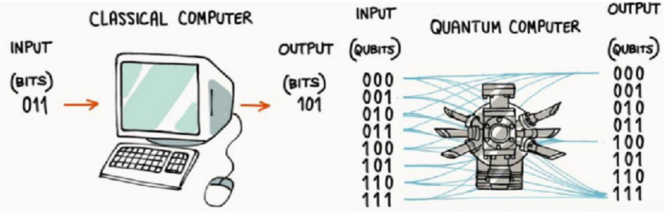
Not performing any measurements, Nature conceals a great deal of *hidden quantum information*, which grows *exponentially* with the number of qubits ($N = 500 > n_{\mathrm{atoms}}$ in the universe !).

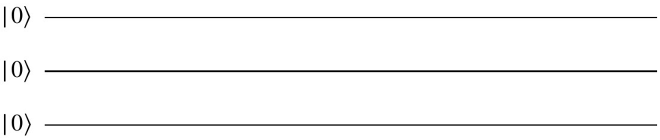
Quantum Computation

Quantum Circuit

Quantum circuit: model of quantum computation

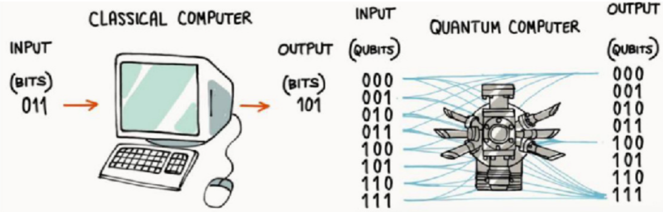
$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

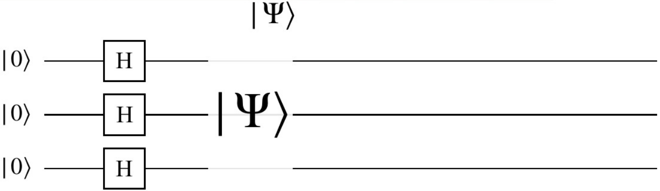




Quantum circuit: model of quantum computation

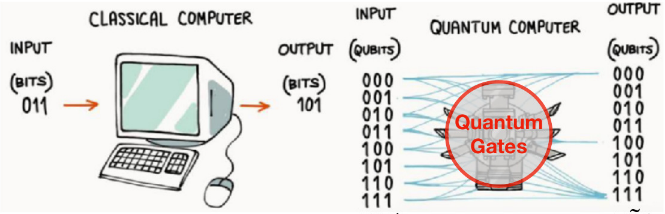
$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

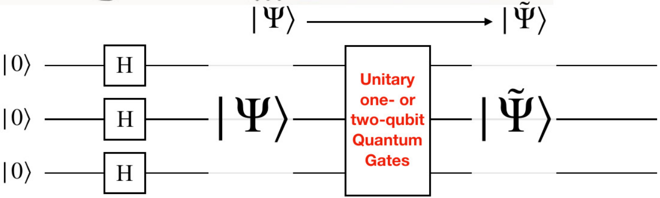




Quantum circuit: model of quantum computation

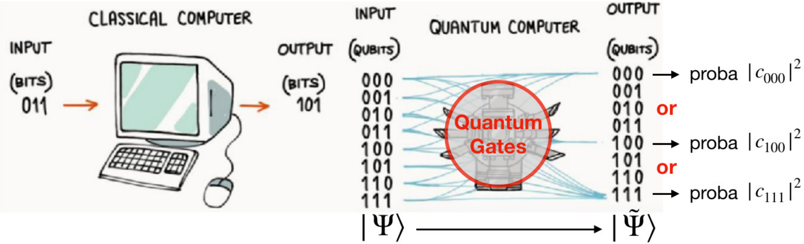
$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$

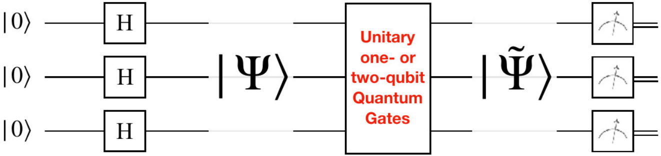




Quantum circuit: model of quantum computation

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right)$$





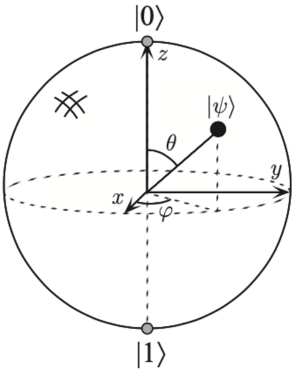
Quantum Computation

Quantum gates

Single-qubit gates: Bloch Sphere representation

Because $(\psi_0, \psi_1) \in \mathbb{C}^2$ and $|\psi_0|^2 + |\psi_1|^2 = 1$, one can rewrite the qubit state as follows:

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



Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a *rotation on the Bloch sphere.* It corresponds to a 2×2 matrix which can be expressed as a function of four basis operators.

Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a *rotation on the Bloch sphere.* It corresponds to a 2×2 matrix which can be expressed as a function of four basis operators.

A commonly used basis consists in *Pauli's matrices*:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Single-qubit gates: Pauli matrices

Any unitary operation $\hat{U}$ on a single qubit might be seen as a *rotation on the Bloch sphere.* It corresponds to a 2×2 matrix which can be expressed as a function of four basis operators.

A commonly used basis consists in *Pauli's matrices*:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Alternative notations:

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Properties: $\hat{X}^2 = \hat{Y}^2 = \hat{Z}^2 = \hat{I}$ and $\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j = i\varepsilon_{ijk}\boldsymbol{\sigma}_k + \delta_{ij}\mathbb{I}$

Single-qubit gates: Pauli generators for rotations

Any rotation around the direction $\vec{n} = (n_x, n_y, n_z)$ ($|\vec{n}| = 1$) can be expressed as the exponential matrix of a superposition of Pauli's matrices, with $\hat{\vec{\sigma}} = (\hat{X}, \hat{Y}, \hat{Z})$,

$$\begin{aligned}
e^{i\frac{\theta}{2}(\vec{n}\cdot\hat{\vec{\sigma}})} &= \sum_{k=0}^{\infty} \frac{i^k \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^k}{k!} \\
&= \sum_{p=0}^{\infty} \frac{(-1)^p \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^{2p}}{(2p)!} + i\sum_{q=0}^{\infty} \frac{(-1)^q \left(\frac{\theta}{2}\vec{n}\cdot\hat{\vec{\sigma}}\right)^{2q+1}}{(2q+1)!} \\
&= \mathbb{I}\sum_{p=0}^{\infty} \frac{(-1)^p \left(\frac{\theta}{2}\right)^{2p}}{(2p)!} + i\left(\vec{n}\cdot\hat{\vec{\sigma}}\right)\sum_{q=0}^{\infty} \frac{(-1)^q \left(\frac{\theta}{2}\right)^{2q+1}}{(2q+1)!} \\
&= \cos\frac{\theta}{2}\mathbb{I} + i\sin\frac{\theta}{2}(n_x\hat{X} + n_y\hat{Y} + n_z\hat{Z}) = R_{\vec{n}}(\theta)
\end{aligned}$$

Single-qubit gates

$$\hat{X} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}, \quad \hat{Z} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{array}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}, \quad \hat{R}_\theta = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \end{array},$$

Single-qubit gates

$$\hat{X} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}, \quad \hat{Z} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{array}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}, \quad \hat{R}_\theta = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \end{array},$$

Alternatively:

$$\hat{X} = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad \hat{H} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|, \quad \hat{R}_\theta = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$$

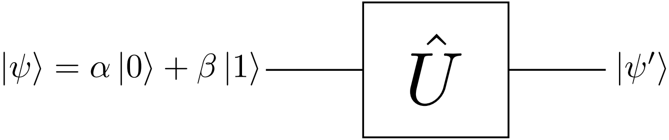
Single-qubit gates

$$\hat{X} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}, \quad \hat{Z} = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{array}, \quad \hat{H} = \frac{1}{\sqrt{2}} \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}, \quad \hat{R}_\theta = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \end{array},$$

Alternatively:

$$\hat{X} = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad \hat{H} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|, \quad \hat{R}_\theta = |0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$$

Circuit representation:



Controlled multi-qubit gate C-U

Single-qubit gates cannot create entanglement, one requires multi-qubit gates.

Controlled multi-qubit gate C-U

Single-qubit gates cannot create entanglement, one requires multi-qubit gates.

Consider a register of N qubits, where a quantum operation $\hat{U}$ is applied to the last $(N-1)$ qubits, controlled by the first qubit.

This gate is called a singly-controlled multi-qubit gate (can be easily generalized to a multi-controlled multi-qubit gate) and is given by

$$\text{C-U} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}^{\otimes^{N-1}} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \hat{U}$$

such that $\hat{U}$ is only applied if the first qubit is in state $|1\rangle$.

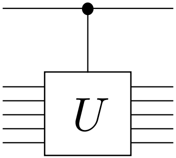
Controlled multi-qubit gate C-U

Single-qubit gates cannot create entanglement, one requires multi-qubit gates.

Consider a register of N qubits, where a quantum operation $\hat{U}$ is applied to the last $(N-1)$ qubits, controlled by the first qubit.

This gate is called a singly-controlled multi-qubit gate (can be easily generalized to a multi-controlled multi-qubit gate) and is given by

$$\text{C-U} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I}^{\otimes^{N-1}} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \hat{U}$$



such that $\hat{U}$ is only applied if the first qubit is in state $|1\rangle$.

Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \color{red}{0} & \color{red}{1} \\ 0 & 0 & \color{red}{1} & \color{red}{0} \end{pmatrix} \end{array}, \quad \text{SWAP} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \color{red}{0} & \color{red}{1} & 0 \\ 0 & \color{red}{1} & \color{red}{0} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}, \quad \text{SWAP} = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Alternatively:

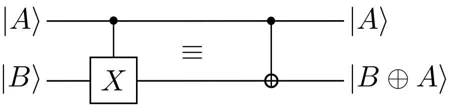
$$|\text{C-NOT}\rangle = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|, \quad |\text{SWAP}\rangle = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$

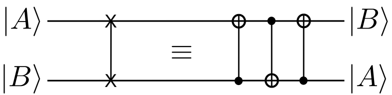
Two-qubit gates

$$\text{C-NOT} = \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \overset{\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array}}{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}, \quad \text{SWAP} = \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \overset{\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array}}{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}$$

Alternatively:

$$|\text{C-NOT}\rangle = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|, \quad |\text{SWAP}\rangle = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$





Toffoli gate

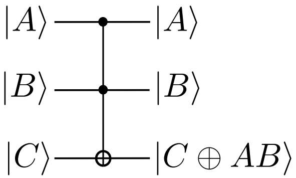
The Toffoli gate is a multi-controlled 3-qubit gate (controlled-controlled NOT gate), which was originally devised as a *universal, reversible classical logic gate* by Toffoli.

$$
\begin{array}{c} \\ |000\rangle \\ |001\rangle \\ |010\rangle \\ |011\rangle \\ |100\rangle \\ |101\rangle \\ |110\rangle \\ |111\rangle \end{array}
\begin{array}{c}
\begin{array}{cccccccc} |000\rangle & |001\rangle & |010\rangle & |011\rangle & |100\rangle & |101\rangle & |110\rangle & |111\rangle \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\end{array}
$$

Toffoli gate

The Toffoli gate is a multi-controlled 3-qubit gate (controlled-controlled NOT gate), which was originally devised as a *universal, reversible classical logic gate* by Toffoli.

	$\lvert 000\rangle$	$\lvert 001\rangle$	$\lvert 010\rangle$	$\lvert 011\rangle$	$\lvert 100\rangle$	$\lvert 101\rangle$	$\lvert 110\rangle$	$\lvert 111\rangle$
$\lvert 000\rangle$	1	0	0	0	0	0	0	0
$\lvert 001\rangle$	0	1	0	0	0	0	0	0
$\lvert 010\rangle$	0	0	1	0	0	0	0	0
$\lvert 011\rangle$	0	0	0	1	0	0	0	0
$\lvert 100\rangle$	0	0	0	0	1	0	0	0
$\lvert 101\rangle$	0	0	0	0	0	1	0	0
$\lvert 110\rangle$	0	0	0	0	0	0	0	1
$\lvert 111\rangle$	0	0	0	0	0	0	1	0



Quantum Computation

Examples

Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

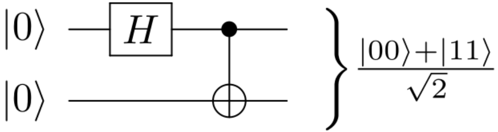
$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

They can be prepared with an Hadamard gate and a CNOT gate:

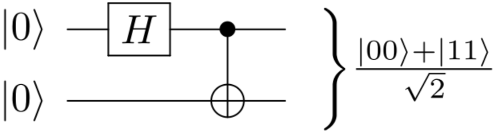


Example 1: Bell states

Bell states, also called EPR states or EPR pairs, are:

$$\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

They can be prepared with an Hadamard gate and a CNOT gate:



$$|00\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \xrightarrow{\text{C-NOT}_{12}} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Einstein, Podolski and Rosen (EPR, 1935)

Quantum mechanics:

1. An *unobserved* particle does no possess physical properties that exist *independent* of observation. Rather, such physical properties *arise as a consequence of measurements* performed upon the system.
2. For an *entangled* state of a composite system of A and B, the action performed on system A will *modify* the description of system B.

Einstein, Podolski and Rosen (EPR, 1935)

Quantum mechanics:

1. An *unobserved* particle does no possess physical properties that exist *independent* of observation. Rather, such physical properties *arise as a consequence of measurements* performed upon the system.
2. For an *entangled* state of a composite system of A and B, the action performed on system A will *modify* the description of system B.

EPR wanted to show that any *complete* physical theory should fulfill the sufficient condition that a value of a physical property can be predicted with certainty immediately **before** measurement.

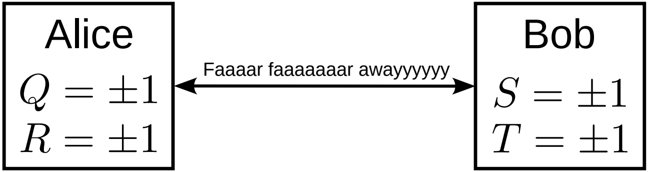
Hence, quantum mechanics is incomplete and one is missing a *local hidden variable*, according to their assumption of *local realism*.

Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).

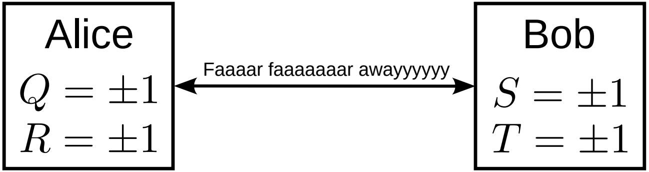
Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).



Bell's inequality (1964)

Bell thought about an experiment that has different outcome if analyzed by our common sense notions of the world, or by quantum mechanics. Charlie prepares two particles, send one to Alice and one to Bob which perform measurements *simultaneously* (physical influences cannot propagate faster than light!).



Bell inequality:

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2$$

And if Charlie prepares two entangled qubits ?

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \frac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \frac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

we have

$$\langle Q \otimes S \rangle_\psi = \langle R \otimes S \rangle_\psi = \langle R \otimes T \rangle_\psi = -\langle Q \otimes T \rangle_\psi = \frac{1}{\sqrt{2}}$$

Bell's inequality (1964)

If Charlie prepares two entangled qubits in the state $|\psi\rangle = \dfrac{|01\rangle - |10\rangle}{2}$, and that

$$Q = Z_1, R = X_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}, T = \frac{Z_2 - X_2}{\sqrt{2}}$$

we have

$$\langle Q \otimes S\rangle_\psi = \langle R \otimes S\rangle_\psi = \langle R \otimes T\rangle_\psi = -\langle Q \otimes T\rangle_\psi = \frac{1}{\sqrt{2}}$$

such that

$$\langle QS\rangle_\psi + \langle RS\rangle_\psi + \langle RT\rangle_\psi - \langle QT\rangle_\psi = 2\sqrt{2} > 2.$$

Hence, the fact that two spatially separate particles can form an *unseparable system violates Bell inequality*.

And indeed, Bell inequality (1964) are not obeyed by Nature (Alain Aspect experiment, 1982).

Example: Quantum teleportation

Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

Example: Quantum teleportation

Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

But:

1. Alice doesn't know the state of the qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
2. She cannot look at it or it will collapse...
3. She can only communicate with Bob once...

Example: Quantum teleportation

Alice and Bob have one qubit each. While together, they generated an EPR pair $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, but they are now separated. Many years later, Bob is hiding and Alice has a mission: deliver a qubit $|\psi\rangle$ to Bob...

But:

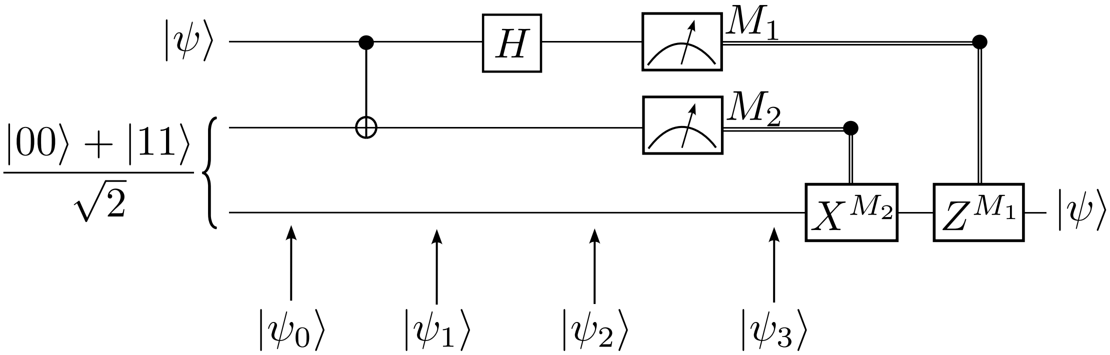
1. Alice doesn't know the state of the qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
2. She cannot look at it or it will collapse...
3. She can only communicate with Bob once...

Fortunately, their EPR pair can be used to send $|\psi\rangle$ to Bob ! (Experiment by Bennett *et al.*, 1993)

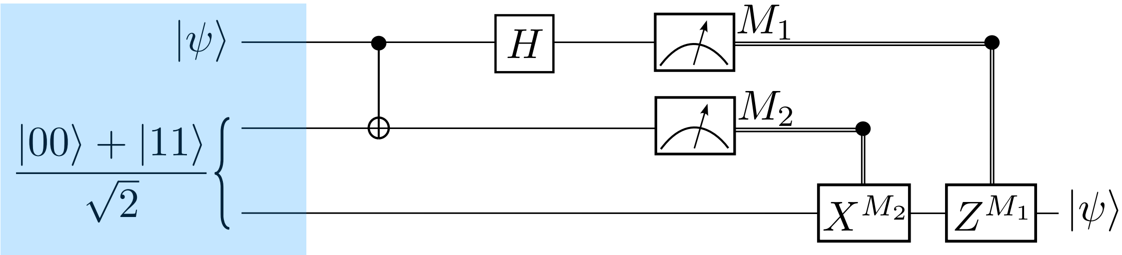
Do we have time to do it together ?

QUIZZ

Example: Quantum teleportation

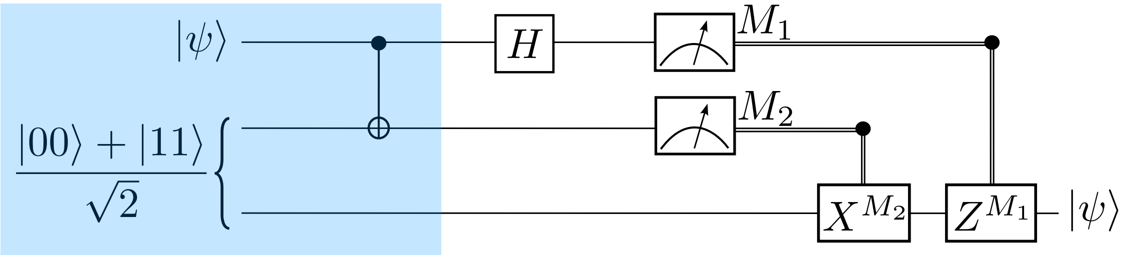


Example: Quantum teleportation



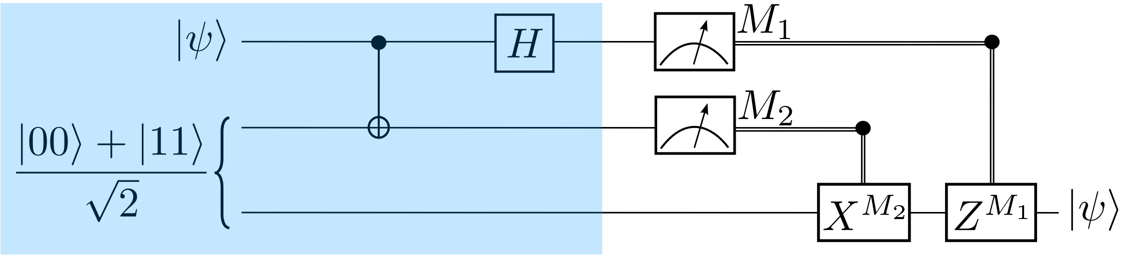
$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\Big)$$

Example: Quantum teleportation



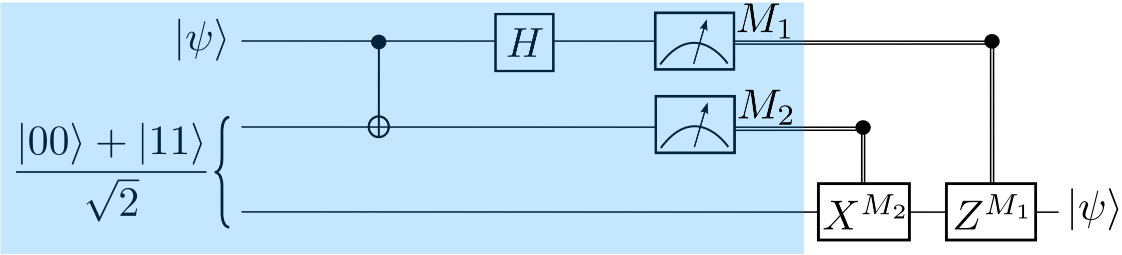
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\Big)$$

Example: Quantum teleportation



$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\Big(\alpha\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \beta\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right)\Big) \\
&= \frac{1}{2}\Big(|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\Big)
\end{aligned}
$$

Example: Quantum teleportation



$$
\begin{array}{rcl}
00 \longrightarrow |\psi_3(00)\rangle & = & \alpha\,|0\rangle + \beta\,|1\rangle \\
01 \longrightarrow |\psi_3(01)\rangle & = & \alpha\,|1\rangle + \beta\,|0\rangle \\
10 \longrightarrow |\psi_3(10)\rangle & = & \alpha\,|0\rangle - \beta\,|1\rangle \\
11 \longrightarrow |\psi_3(11)\rangle & = & \alpha\,|1\rangle - \beta\,|0\rangle
\end{array}
$$

Example: Quantum teleportation

Only the information about the quantum state and not the state itself (no matter or energy) passes from Alice to Bob.

The teleportation is not faster than light, as Alice has to pass the information to Bob by a classical channel.

Classical versus Quantum

QUIZZ

Irreversibility versus Reversibility

Quantum gates are *unitary*, and hence *reversible*.

Irreversibility versus Reversibility

Quantum gates are *unitary*, and hence *reversible*.

Classical logical gates are not all reversible, but *any* irreversible classical algorithm can be transformed into a reversible algorithm at the expense of having a higher volume of information and the introduction of the *Toffoli* gate.

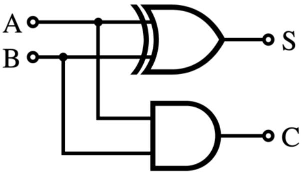
Irreversibility versus Reversibility

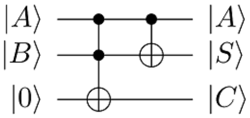
Quantum gates are *unitary*, and hence *reversible*.

Classical logical gates are not all reversible, but *any* irreversible classical algorithm can be transformed into a reversible algorithm at the expense of having a higher volume of information and the introduction of the *Toffoli* gate.

Toffoli gate is a *universal reversible* gate for classical computing. As it is reversible, it has a quantum analog, and any classical algorithm has a quantum analog as well.

Example of the half-adder circuit:





Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Quantum computing:

1. Toffoli + non trivial single-qubit gate
2. CNOT, rotation gates $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$
3. Clifford (CNOT + S + H) + T gates

Universal operations

'Universal' refers to the fact that any gate can be implemented by using only successions of these gates.

Classical computing: NAND or NOR or Toffoli are universal gates.

Quantum computing:

1. Toffoli + non trivial single-qubit gate
2. CNOT, rotation gates $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$
3. Clifford (CNOT + S + H) + T gates

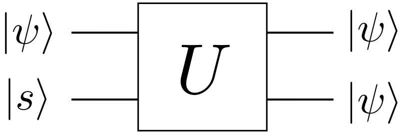
Note: quantum algorithms that is written with Clifford gates can be simulated *efficiently* on classical computers.

Non-Clifford relative phase gates are very important ! (Phase-shift gate, S gate, T gate, ...)

Making copy ? No cloning theorem

Copies are *everywhere* in the classical world, they are one of the most *powerful* means of spreading and preserving information.

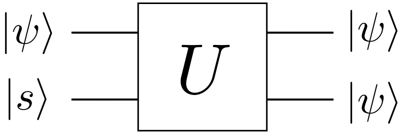
Can we make a copy of an *unknown* quantum state ?



Making copy ? No cloning theorem

Copies are *everywhere* in the classical world, they are one of the most *powerful* means of spreading and preserving information.

Can we make a copy of an *unknown* quantum state ?



Suppose the procedure works for two particular pure states $|\psi\rangle$ and $|\varphi\rangle$, thus

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\,, \qquad U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

The inner product of the two states give $\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \longrightarrow |\psi\rangle$ and $|\varphi\rangle$ are either equal or orthogonal.

Hence, a general quantum cloning device is **impossible**.

Take Home Messages

Take Home messages

Quantum computing differs from classical computing due to:

- Superposition
- Entanglement
- Measurement (collapse)
- No-cloning
- Reversibility (unitary operations)

Developing *efficient* quantum algorithms for practical relevant (industrial or societal) tasks is not trivial, as it requires a radical change of vision of computing.

References

Nielsen, M., and Chuang, I. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press.

Kenneth Maussang, Université de Montpellier, Introduction to quantum computing

Y. Leroyer et G. Sénizergues 1 ENSEIRB-MATMECA, Introduction à l'information quantique

Wikipedia

Institut Charles Gerhardt Montpellier

CHEMISTRY: MOLECULES TO MATERIALS