Introduction to Quantum information and Computation

Germán Sierra (Instituto de Física Teórica UAM-CSIC, Madrid)

6th INFIERY Summer School
Madrid, 1st September 2021

Plan of the lecture

- **Part I: Historial background**

- **Part II: The qubit and quantum gates**

Quantum Computation
and
Quantum Information

Quantum Mechanics

Quantum Computation
and
Quantum Information

Quantum Mechanics

Computer Sciences

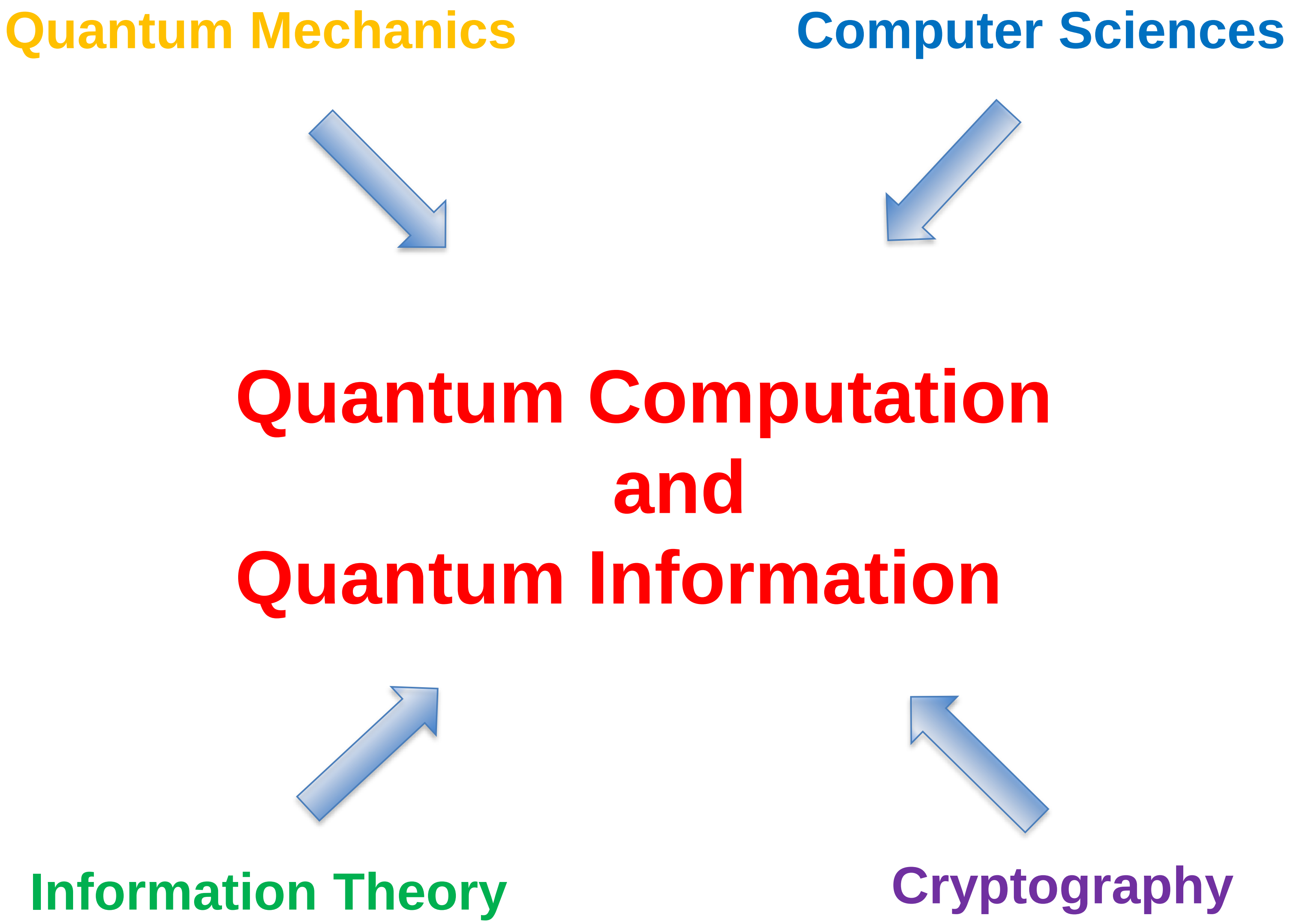
Quantum Computation
and
Quantum Information

Quantum Mechanics

Computer Sciences

Quantum Computation
and
Quantum Information

Information Theory


Quantum Mechanics
Computer Sciences
Quantum Computation
and
Quantum Information
Information Theory
Cryptography

Quantum Mechanics

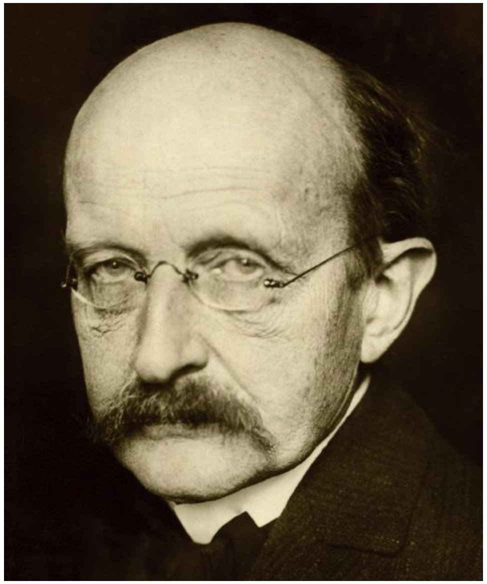
Quantum Mechanics

Golden age of Physics

Quantum Mechanics

Golden age of Physics

First Quantum Revolution



Max Planck
1858 - 1947

Ueber eine Verbesserung der Wien'schen Spectralgleichung; von M. Planck.

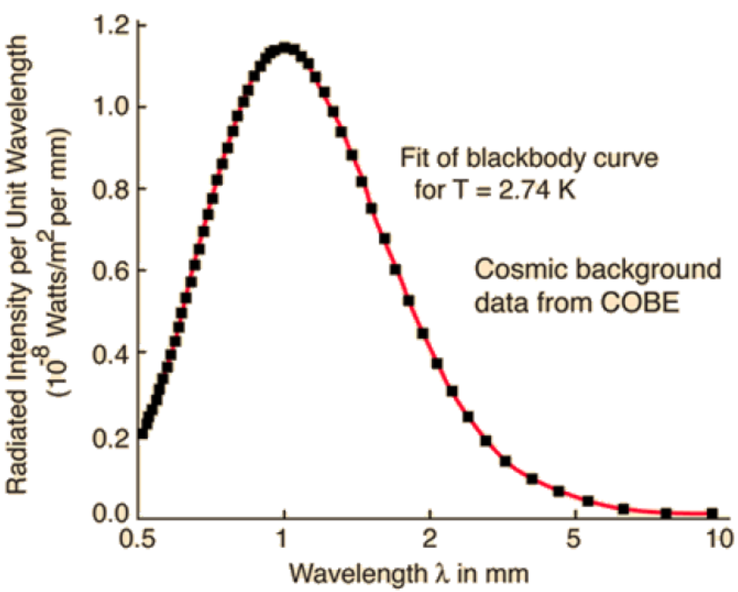
(Vorgetragen in der Sitzung vom 19. October 1900.)

About an improvement of Wien's spectral equation

Zur Theorie des Gesetzes der Energieverteilung im Normalspectrum; von M. Planck.

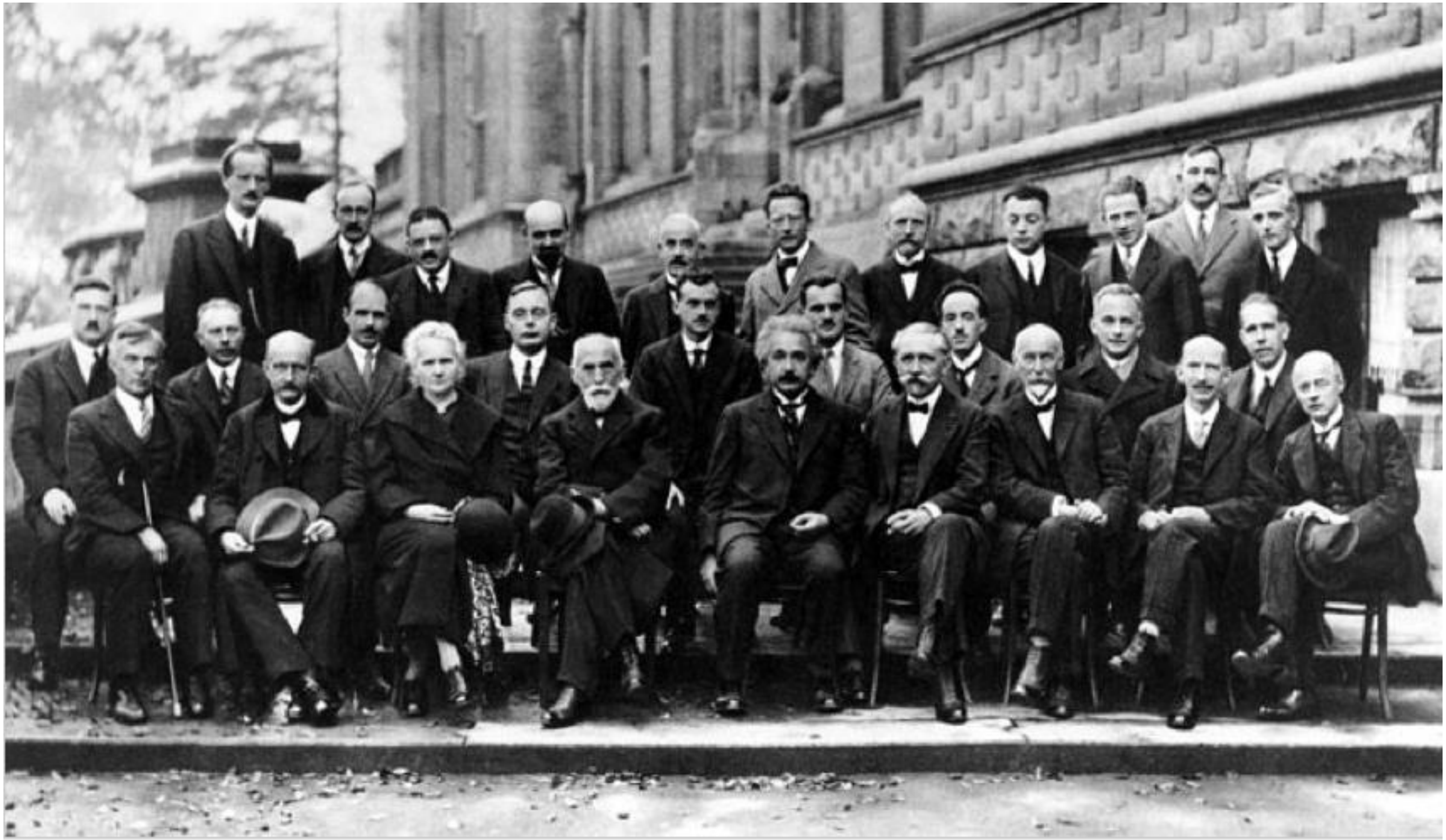
(Vorgetragen in der Sitzung vom 14. December 1900.)

On the theory of the law of energy distribution in normal spectrum



$$u_\nu \, d\nu = \frac{8\pi h \nu^3}{c^3} \cdot \frac{d\nu}{e^{\frac{h\nu}{k\vartheta}} - 1}$$

V-Solvay conference “electrons et photons” (1927)

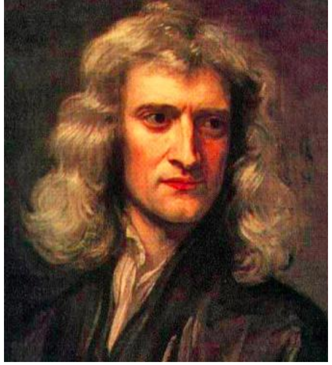


A. Piccard, E. Henriot, P. Ehrenfest, E. Herzen, Th. de Donder, E. Schrödinger, J.E. Verschaffelt, W. Pauli, W. Heisenberg, R.H. Fowler, L. Brillouin;

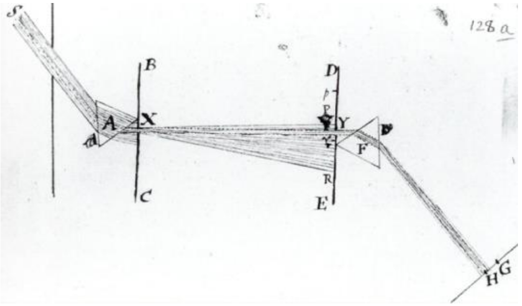
P. Debye, M. Knudsen, W.L. Bragg, H.A. Kramers, P.A.M. Dirac, A.H. Compton, L. de Broglie, M. Born, N. Bohr;
I. Langmuir, M. Planck, M. Skłodowska-Curie, H.A. Lorentz, A. Einstein, P. Langevin, Ch.-E. Guye, C.T.R. Wilson, O.W. Richardson

is light
a wave or a particle?

is light
a wave or a particle?

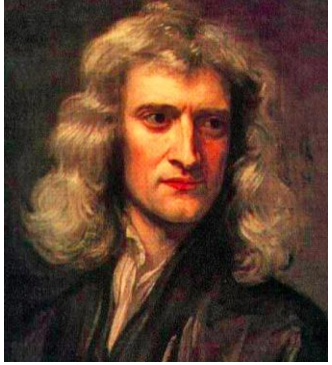


Isaac Newton
1642-1727

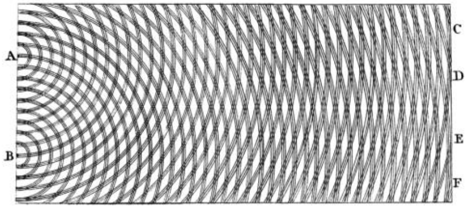


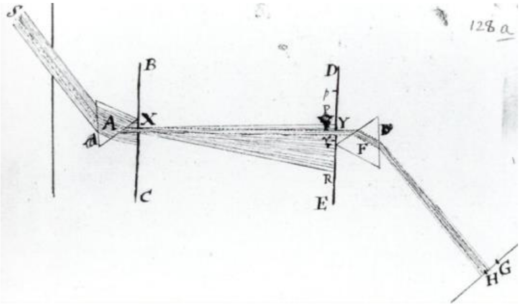
Thomas Young
1773-1829

is light
a wave or a particle?



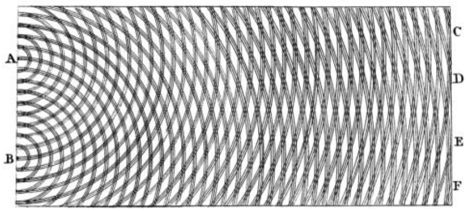
Isaac Newton
1642-1727



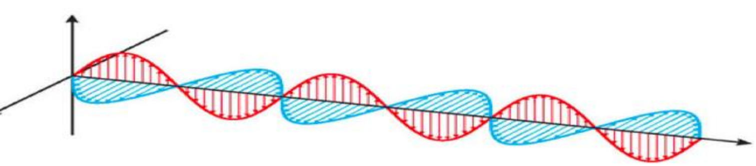


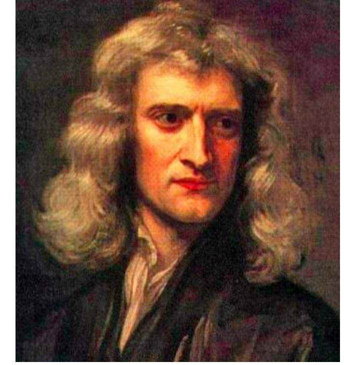
is light a wave or a particle?

Thomas Young
1773-1829

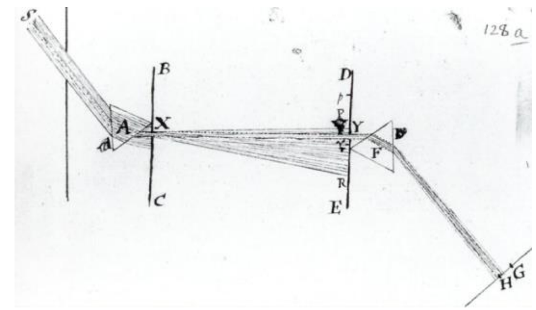


James Maxwell
1831-1879



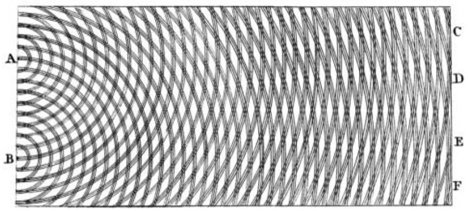


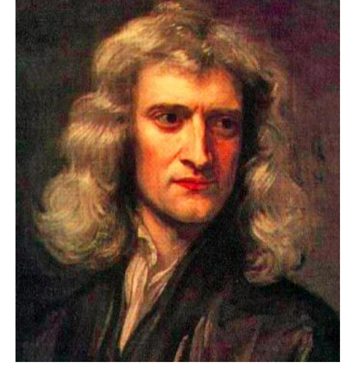
Isaac Newton
1642-1727



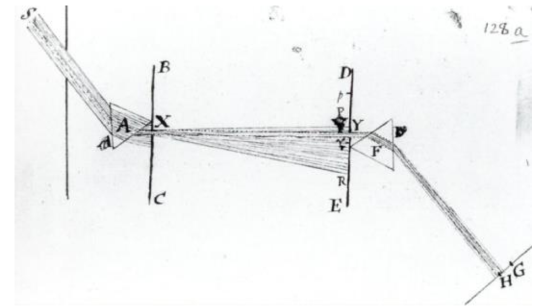
is light
a wave or a particle?

Thomas Young
1773-1829

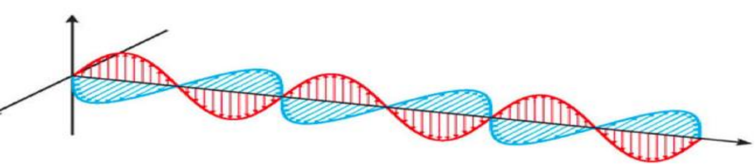




Isaac Newton
1642-1727



James Maxwell
1831-1879



Albert Einstein (1879-1955)

On a heuristic point of view about the creation and generation of light

132

Annalen der Physik, 1905

6. *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt;*
von A. Einstein.

Zwischen den theoretischen Vorstellungen, welche sich die Physiker über die Gase und andere ponderable Körper gebildet haben, und der Maxwellschen Theorie der elektromagnetischen Prozesse im sogenannten leeren Raume besteht ein tiefgreifender formaler Unterschied. Während wir uns nämlich den Zustand eines Körpers durch die Lagen und Geschwindigkeiten einer zwar sehr großen, jedoch endlichen Anzahl von Atomen und Elektronen für vollkommen bestimmt ansehen, bedienen wir uns zur Bestimmung des elektromagnetischen Zustandes eines Raumes kontinuierlicher räumlicher

when a ray of light propagates from a point,
energy is not distributed continuously over increasing volume,
but it is composed of a finite number of energy quanta,
in space,that move without being divided
and that they can be absorbed or emitted only as a whole.

On a heuristic point of view about the creation and generation of light

Annalen der Physik, 1905

6. *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt;*

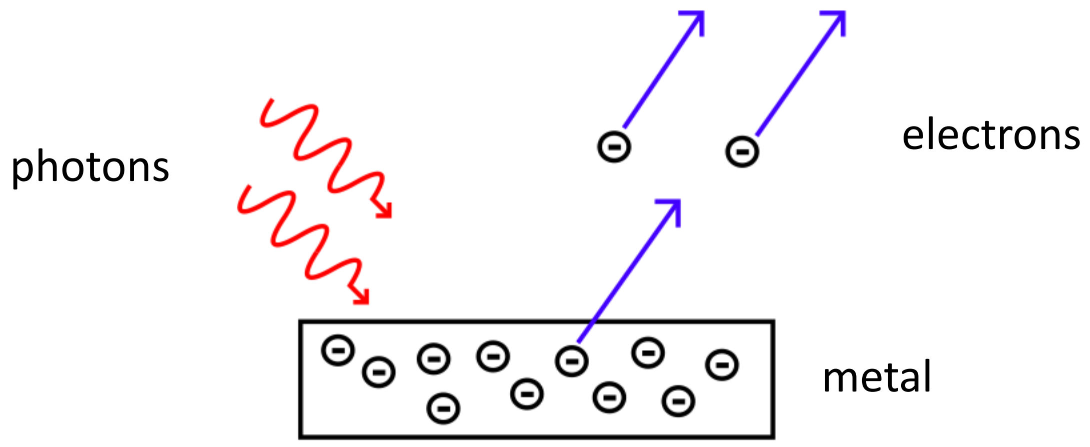
von A. Einstein.

Zwischen den theoretischen Vorstellungen, welche sich die Physiker über die Gase und andere ponderable Körper gebildet haben, und der Maxwellschen Theorie der elektromagnetischen Prozesse im sogenannten leeren Raume besteht ein tiefgreifender formaler Unterschied. Während wir uns nämlich den Zustand eines Körpers durch die Lagen und Geschwindigkeiten einer zwar sehr großen, jedoch endlichen Anzahl von Atomen und Elektronen für vollkommen bestimmt ansehen, bedienen wir uns zur Bestimmung des elektromagnetischen Zustandes eines Raumes kontinuierlicher räumlicher

when a ray of light propagates from a point,
energy is not distributed continuously over increasing volume,
but it is composed of a finite number of energy quanta,
in space,that move without being divided
and that they can be absorbed or emitted only as a whole.

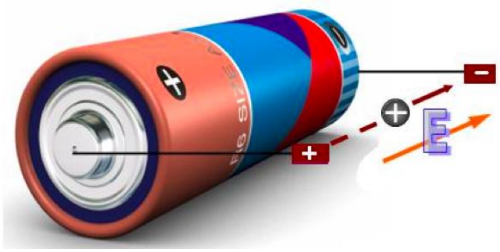
Quantum of light = photon

Photoelectric effect



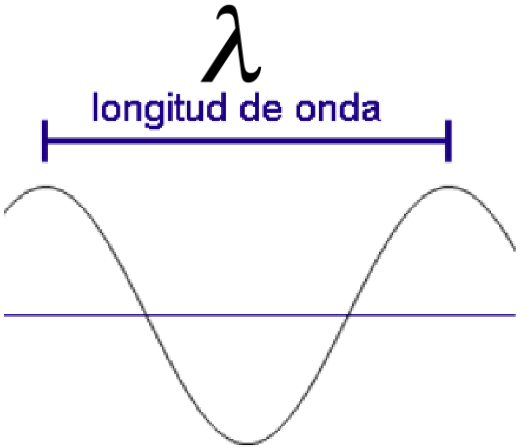
$$E = h\,f$$ (Planck 1900)

Energy of a yellow photon $E \approx 2$ electrón-voltios



Particles are also waves

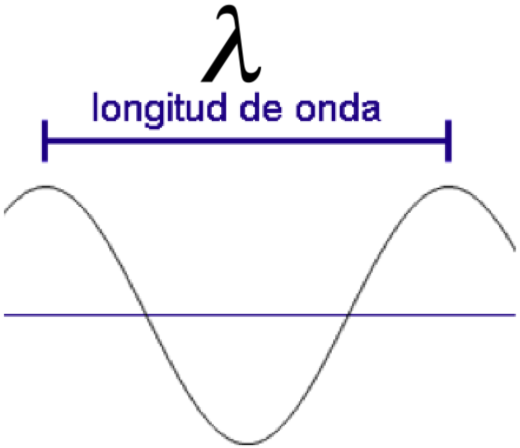
Louis de Broglie
1892-1987



$$\lambda = \frac{h}{p}$$

Louis de Broglie
1892-1987

Particles are also waves



$$\lambda = \frac{h}{p}$$

Werner Heisenberg
1901- 1976

Matrix Mechanics / uncertainty principle

$$[x, p] = i\,\hbar \qquad \Delta x \Delta p \geq \frac{\hbar}{2}$$

Erwin Schrödinger
1887 - 1961

Wave function / Time evolution

$$i \frac{\partial \psi}{\partial t} = \left(-\frac{\hbar^2 \nabla^2}{2m} + V(\vec{x}) \right) \psi$$

Erwin Schrödinger
1887 - 1961

Max Born
1882 - 1970

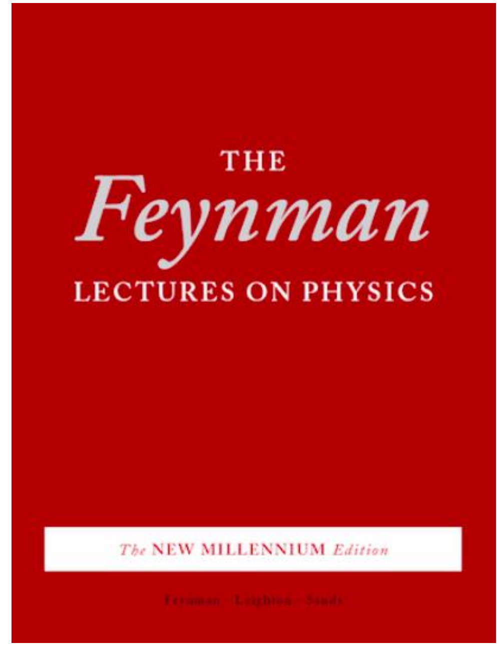
Wave function / Time evolution

$$i\,\frac{\partial\psi}{\partial t} = \left(-\frac{\hbar^2\nabla^2}{2m} + V(\vec{x})\right)\psi$$

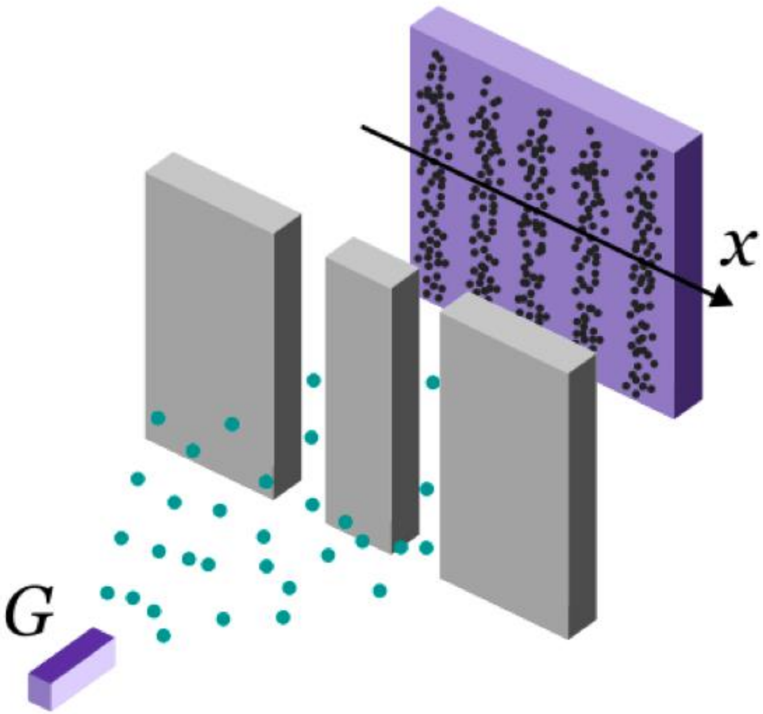
Probabilistic interpretation

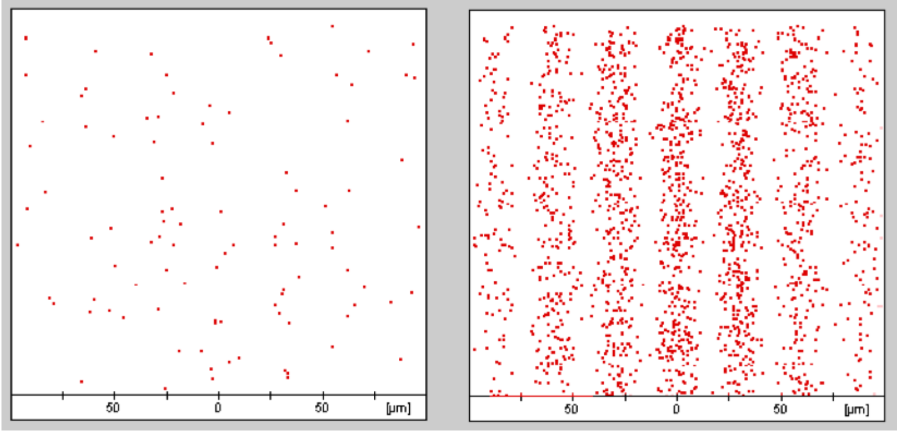
$$\frac{dP}{dV} = |\psi(\vec{x})|^2$$

Richard Feymann : ***Quantum Mechanics can be understood by giving it a lot of thought***
1918 - 1988 ***to the double slit experiment***

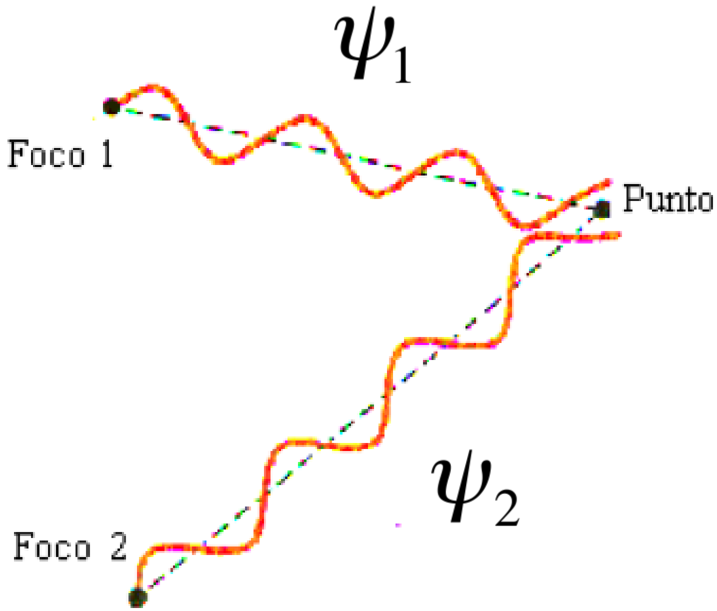


Double slit experiment with electrons

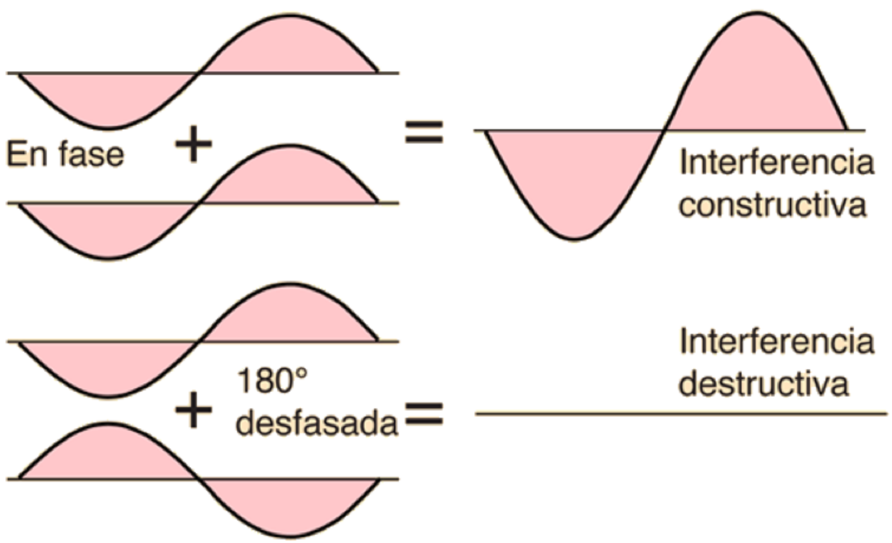




Interference and superposition principle



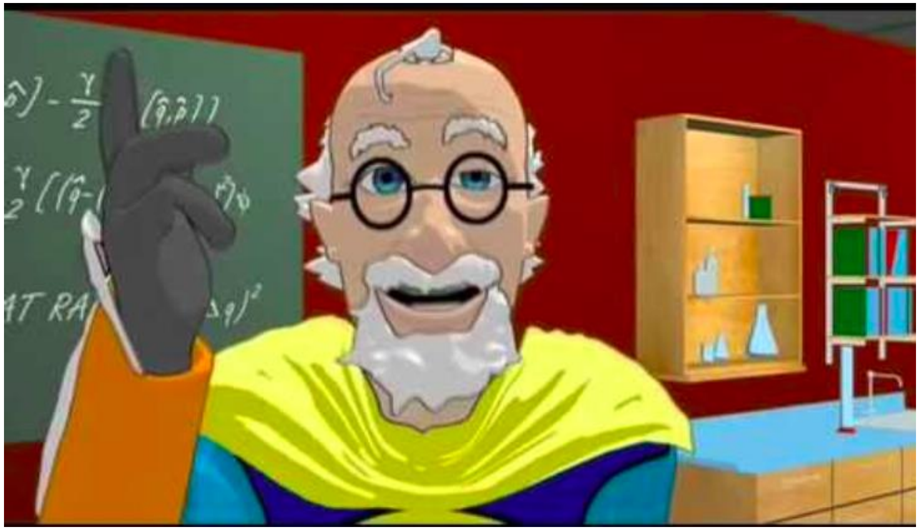
$$\psi_1 + \psi_2$$



See in YouTube

Dr. Quantum – Double Slit experiment

https://www.youtube.com/watch?v=rQJ4yX1l6to



Paradox: the electron "passes" through both slits
INTERFERING WITH ITSELF

“Quantum” Skier

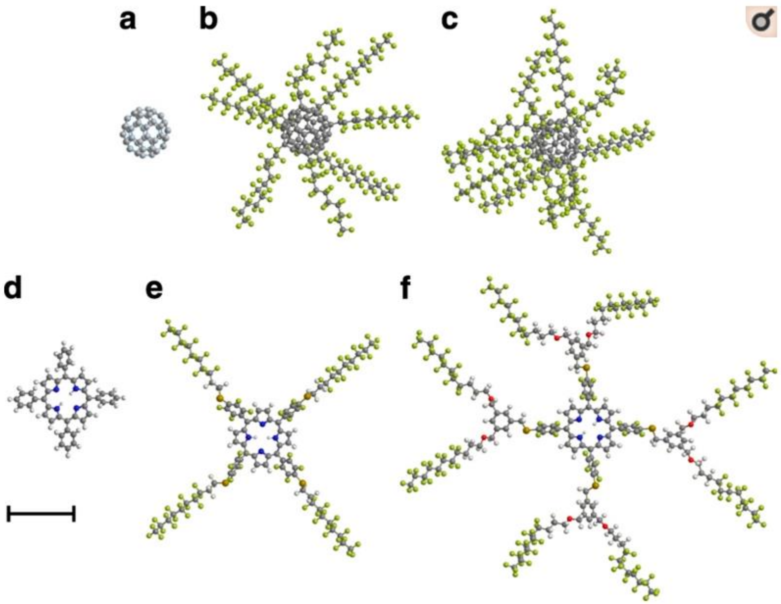
Classical Observer

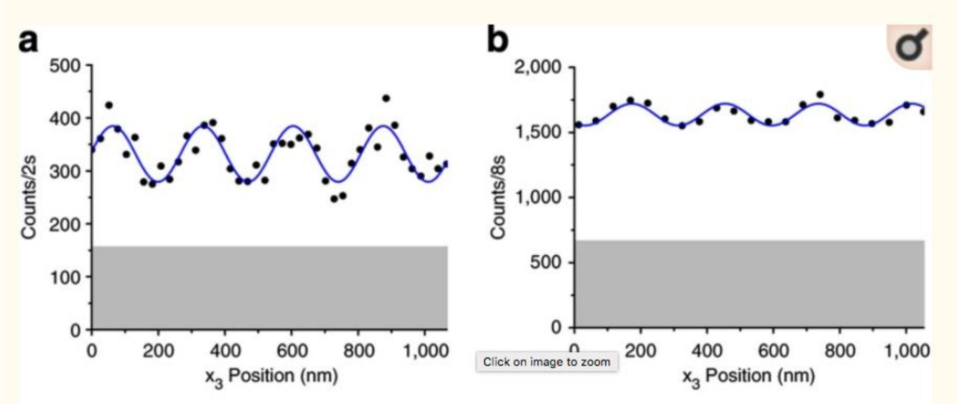
Nat Commun. 2011 Apr; 2: 263.
Published online 2011 Apr 5. doi: 10.1038/ncomms1263

PMCID: PMC3104521
PMID: 21468015

Quantum interference of large organic molecules

Stefan Gerlich,[1] Sandra Eibenberger,[1] Mathias Tomandl,[1] Stefan Nimmrichter,[1] Klaus Hornberger,[2] Paul J. Fagan,[3] Jens Tüxen,[4] Marcel Mayor,[4,5] and Markus Arndt[a,1]

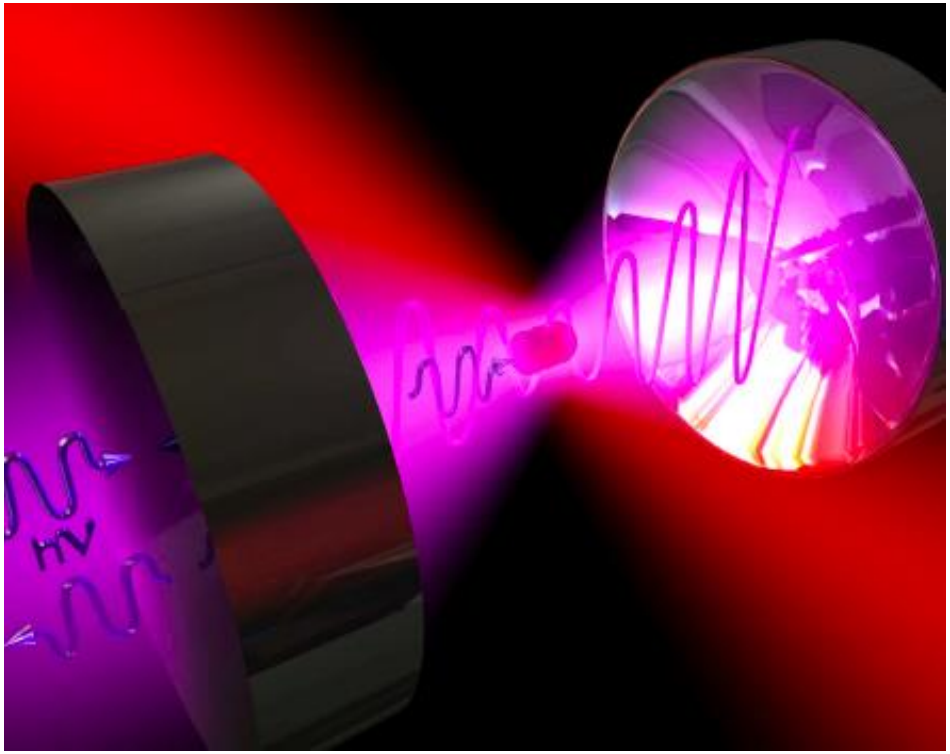




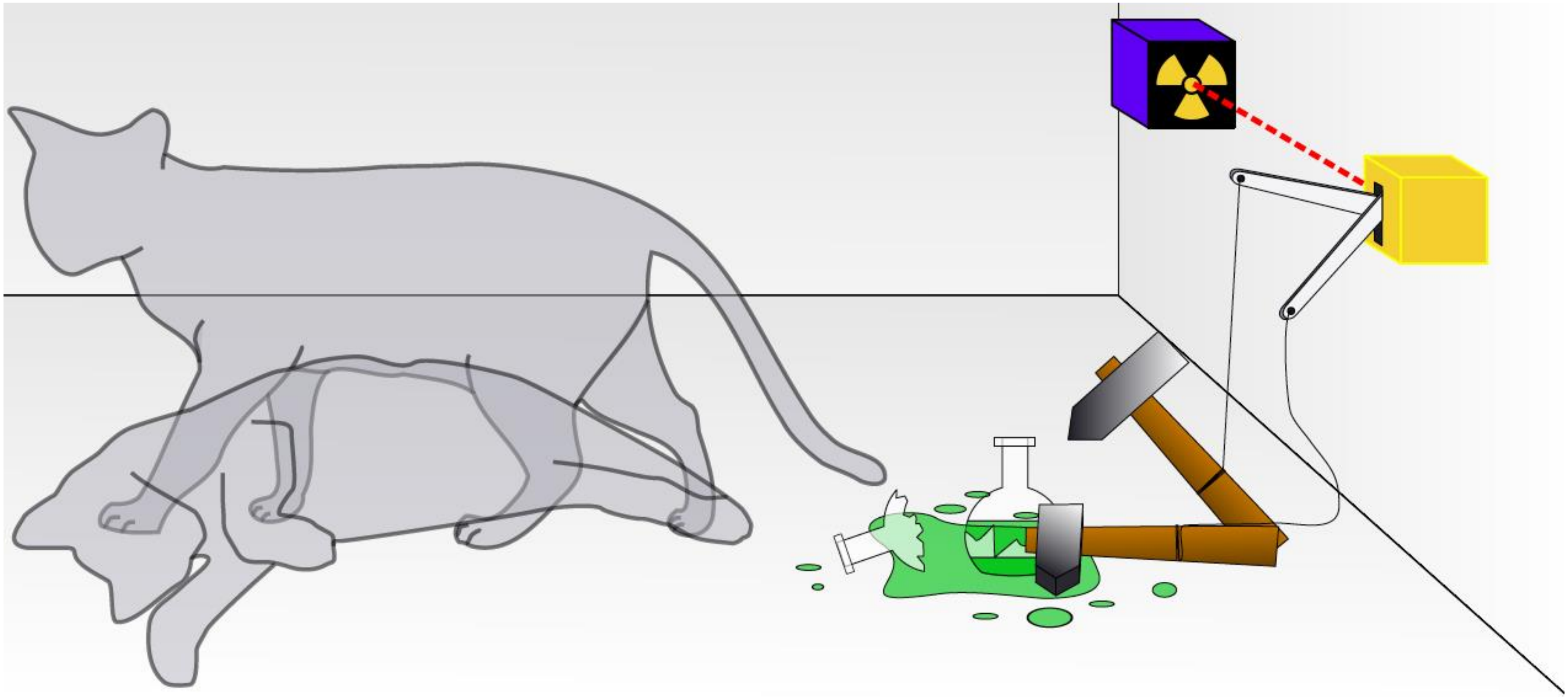
Toward Quantum Superposition of Living Organisms (2010)

Oriol Romero-Isart[1], Mathieu L. Juan[2], Romain Quidant[2,3], and J. Ignacio Cirac[1]

Protocol to create superposition of macroscopic objects including living beings.
Explore the role of life and consciousness in Quantum Mechanics.



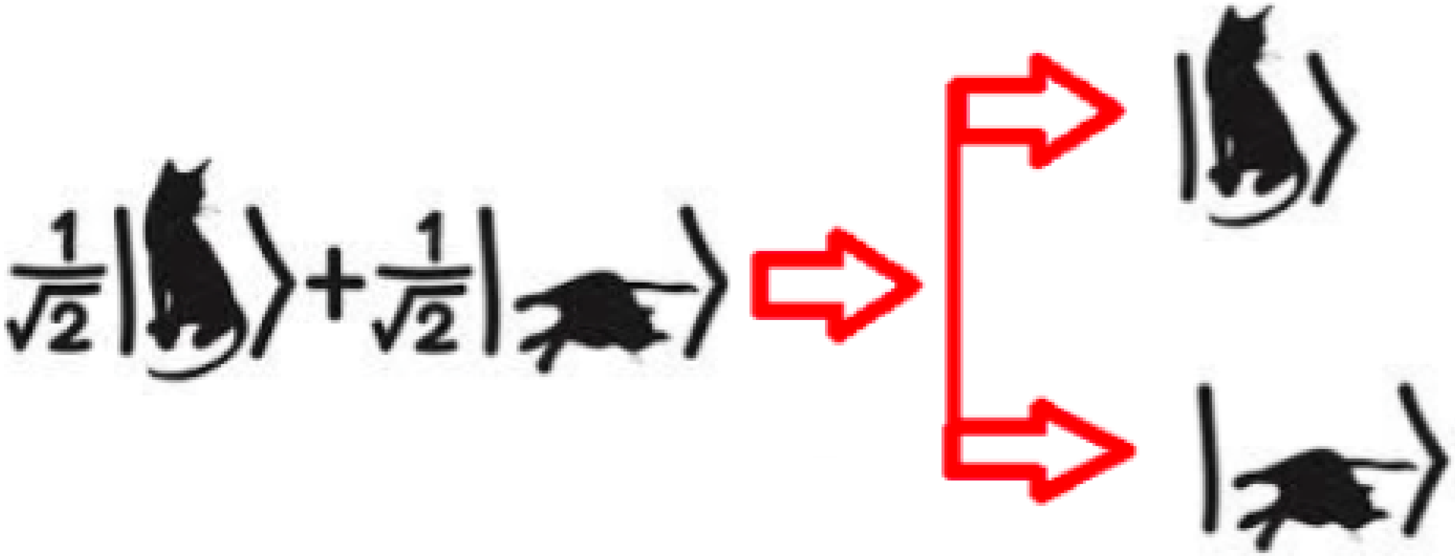
Paradox: Schrödinger cat (1935)



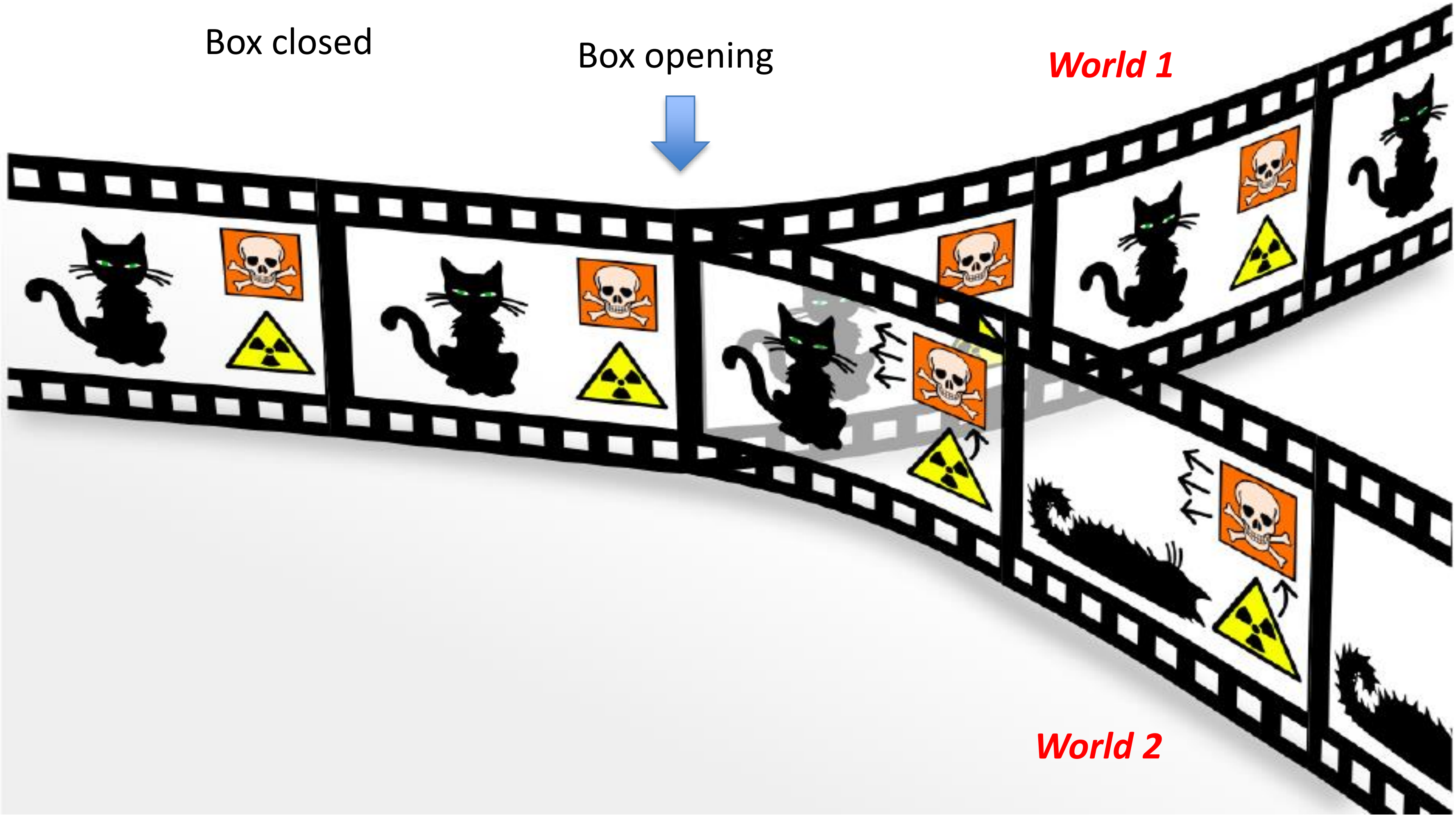
$$\psi = \mathit{Dead} + \mathit{Alive}$$

Copengahen interpretation

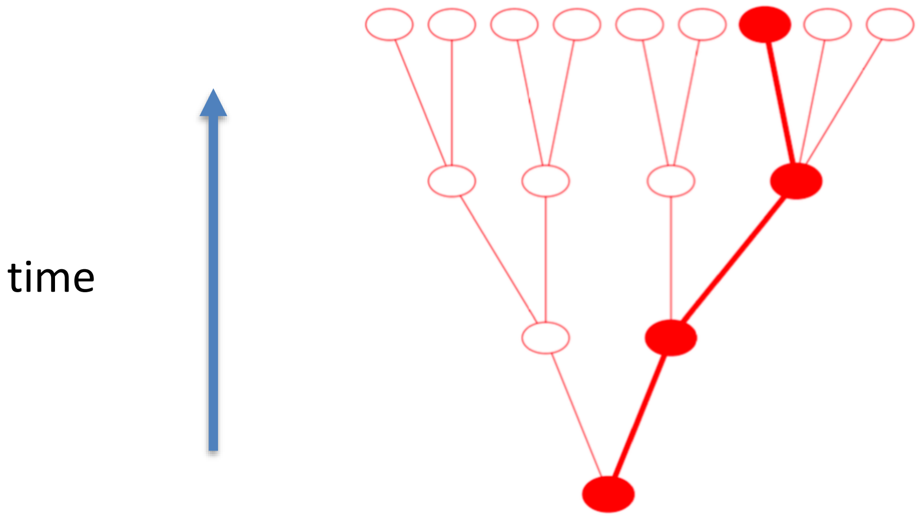
Opening the box produces the COLLAPSE of the wave function



Many world interpretation

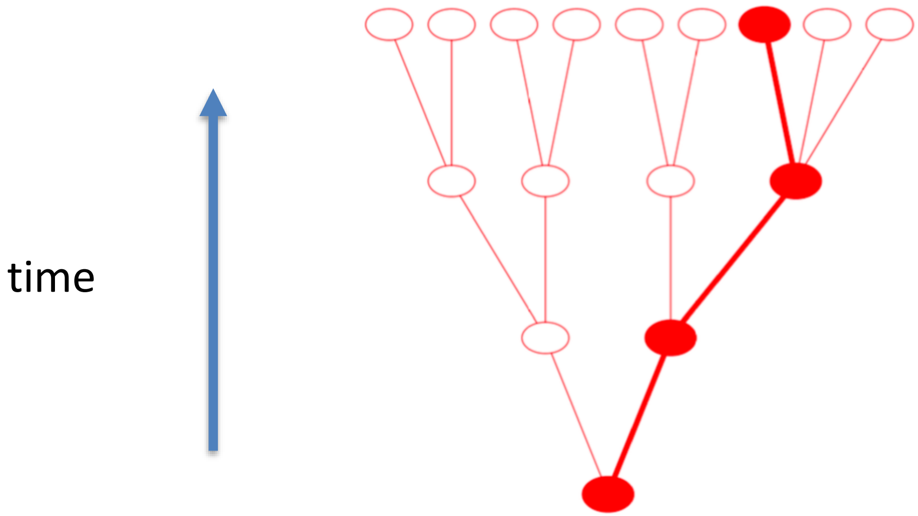


Many world interpretation: Hugh Everett (1957)



Hugh Everett
1930 - 1982

Many world interpretation: Hugh Everett (1957)



Hugh Everett
1930 - 1982

Anticipated in literature by Jorge Luis Borges

in the story "The Garden of Forking Paths" (1941)

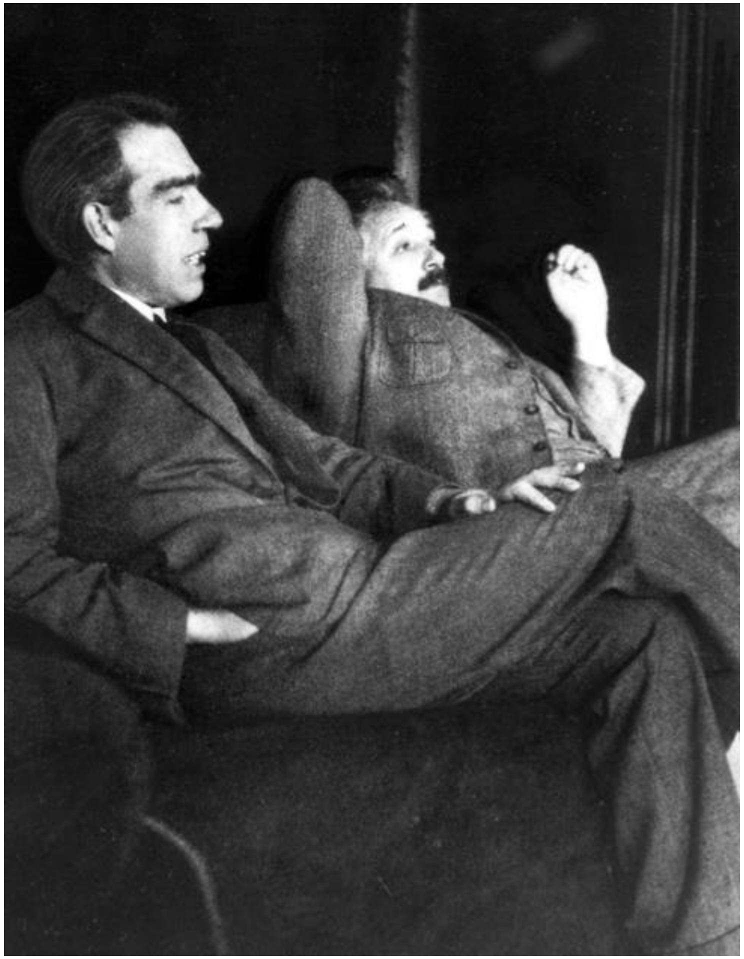
“El jardín de senderos que se bifurcan”

“Unlike Newton and Schopenhauer, his ancestor did not believe in a uniform, absolute time. He believed in infinite series of times, in a growing and dizzying network of divergent, convergent and parallel times….”

Jorge Luis Borges
1899 - 1966

Einstein: I am convinced that God does not play dice.
Do you think the moon is not there when we are not looking at it?

Bohr: Don't tell God what to do



Einstein and Bohr
1925

Einstein, Podolsky and Rosen paradox (1935)

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

New York Times in May of 1935

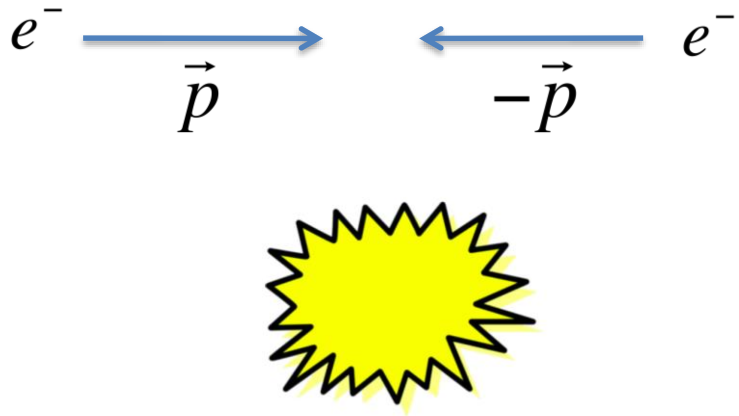
EINSTEIN ATTACKS QUANTUM THEORY

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

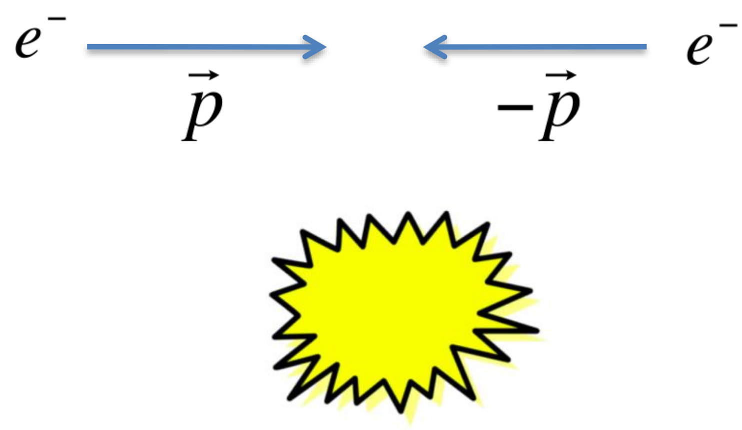
SEE FULLER ONE POSSIBLE

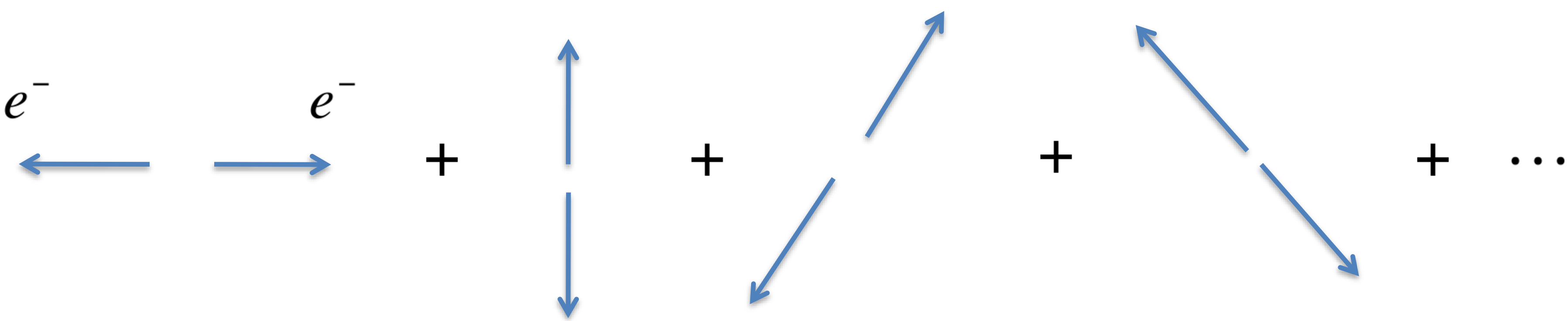
Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

EPR : Gedanken experiment



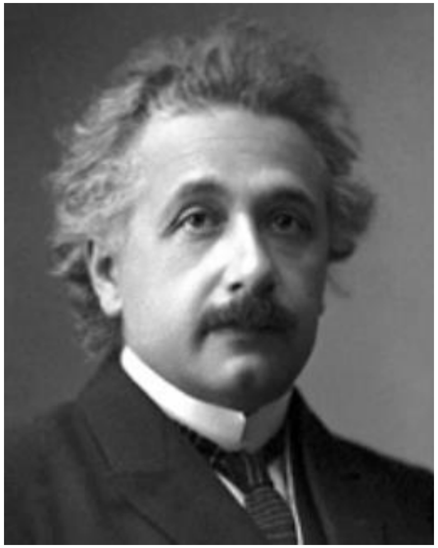
EPR : Gedanken experiment

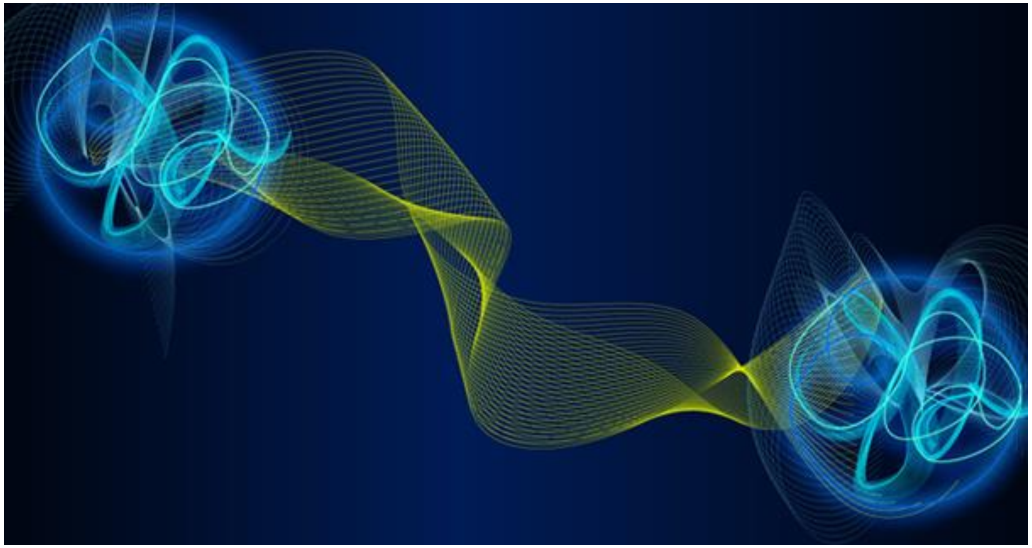




Superposition of two electron with opposite momentum

Spooky action at a distance

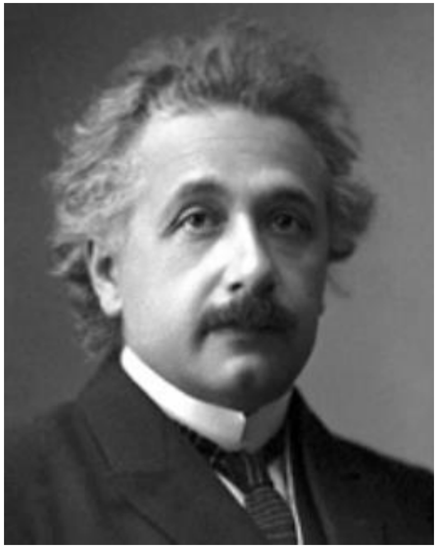


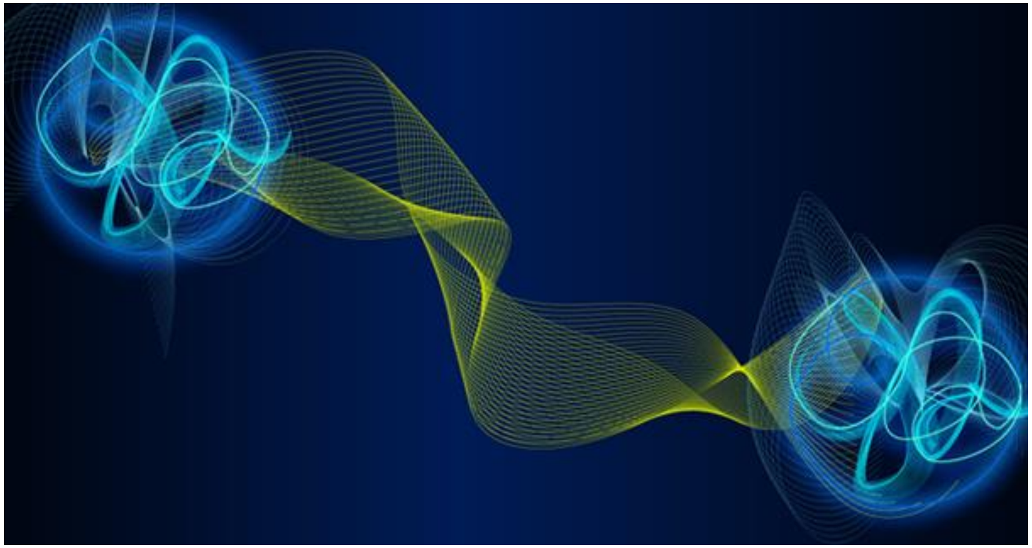


end of the
EPR article

We leave open the possibility that it exists, or not,
a complete description of reality.
We believe that theory exists.

Spooky action at a distance





End of the
EPR article

We leave open the possibility that it exists, or not,
a complete description of reality.
We believe that theory exists.

Hidden variable theories

Schrödinger called entanglement
this instantaneous action at a distance (1935)

Verschränkung (german)

Entanglement is not one, but the characteristic feature of Quantum Mechanics, which imposes its total departure from classical Physics

David Bohm
1917-1992

The EPR paradox spurred the construction
of hidden variable theories

Theory of “pilot waves” of de Broglie and Bohm

David Bohm
1917-1992

The EPR paradox spurred the construction of hidden variable theories

Theory of “pilot waves” of de Broglie and Bohm

John von Neumann
1903-1957

Von Neumann theorem:

Hidden variable theories are incompatible with Quantum Mechanics

Two interpretations of the physical reality

Local Realism (EPR-hidden variables)

The observable quantities have a value prior to their measurement

Quantum Mechanics

The observable quantities DO NOT have a value prior to their measurement

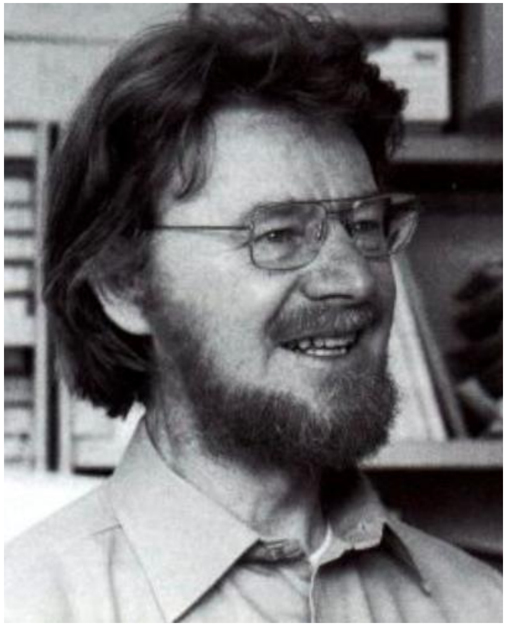
After this discussion a DICTUM was imposed

“Shut up and calculate”

After this discussion a DICTUM was imposed

“Shut up and calculate”

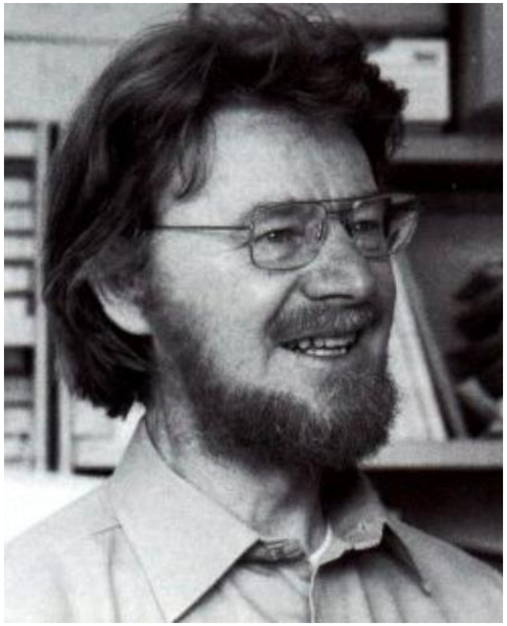
but one should



John Bell
1928-1990

John Bell found that von Neumann's proof was wrong: he assumed what he wanted to prove

EPR ideas were not a mere philosopical speculation about the interpretation of Quantum Mechanics



John Bell
1928-1990

John Bell found that von Neumann's proof was wrong:
he assumed what he wanted to prove

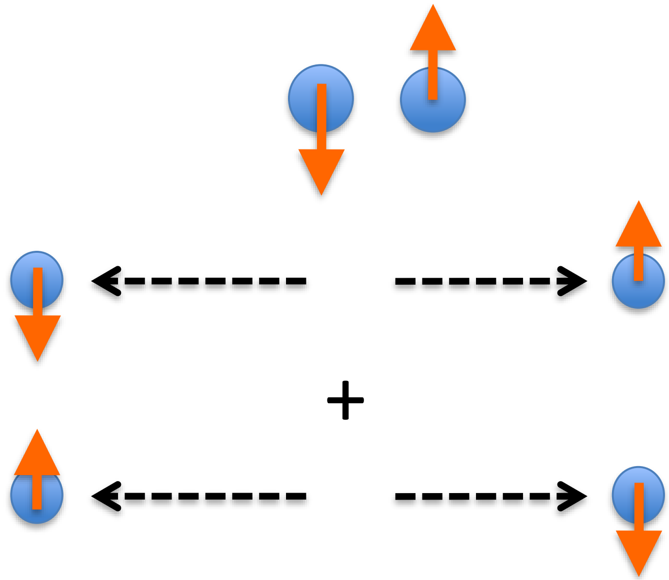
EPR ideas were not a mere philosopical speculation
about the interpretation of Quantum Mechanics

It would be possible to falsify "local realism" with an experiment

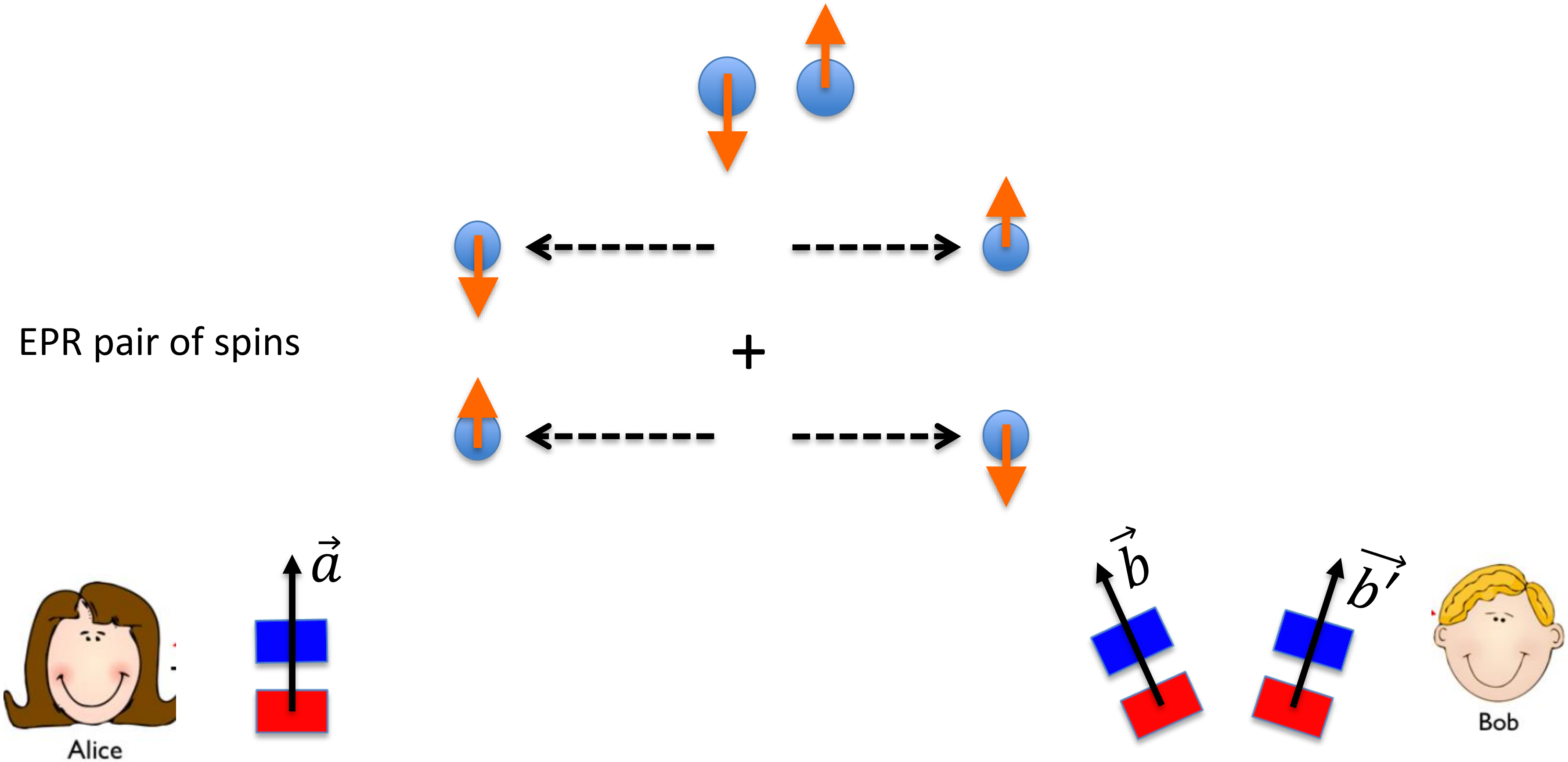
Bell inequalities (1964)

Bell experiment

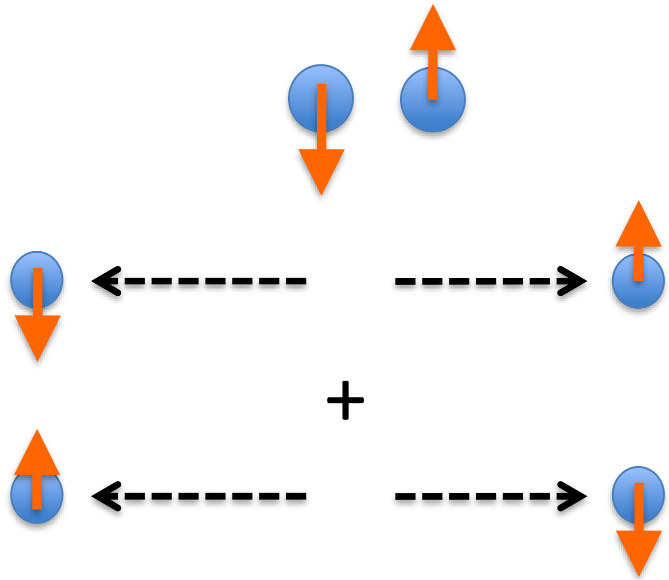
EPR pair of spins



Bell experiment



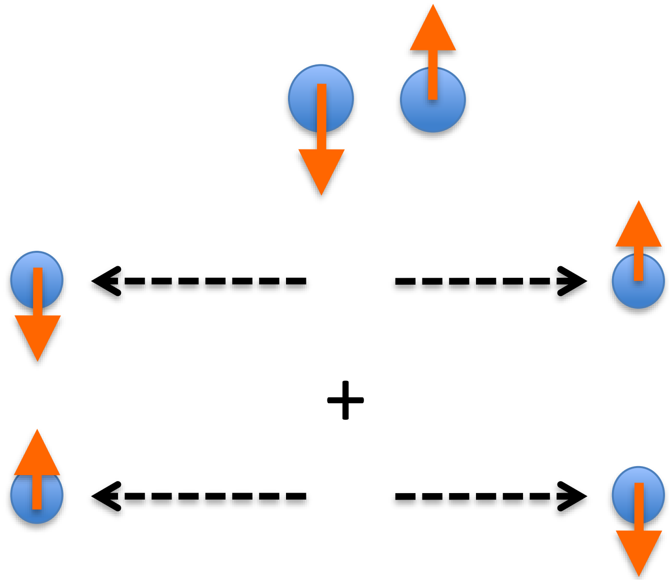
Bell experiment



EPR pair of spins

Local realism ⟹ $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{b}')| \leq 1 + P(b,\vec{b}')$

Bell experiment



EPR pair of spins

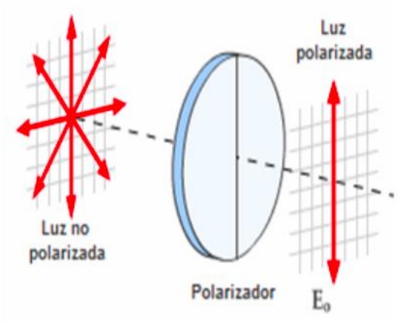
Local realism ⟹ $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{b}')| \leq 1 + P(b,\vec{b}')$

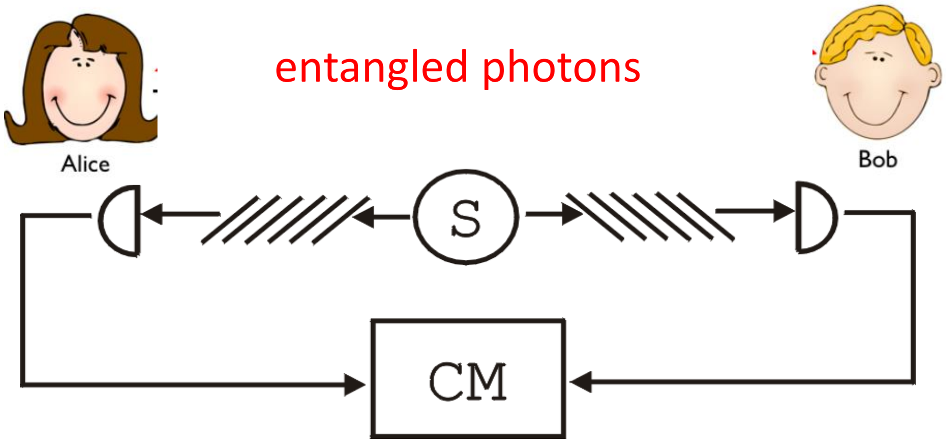
Quantum Mechanics $P\left(\vec{a},\vec{b}\right) = -\vec{a} \cdot \vec{b}$ can violate this inequality

Experiments to verify Bell's inequality

- electrons -> photons

- spin -> polarization





Monitor of coincidences

Aspect's experiments (1981)

CHSH inequality $$-2 \leq S \leq 2$$

Quantum prediction $$S_{MC} = 2.70 \pm 0.05$$

Experimental result $$S_{\exp} = 2.697 \pm 0.01$$

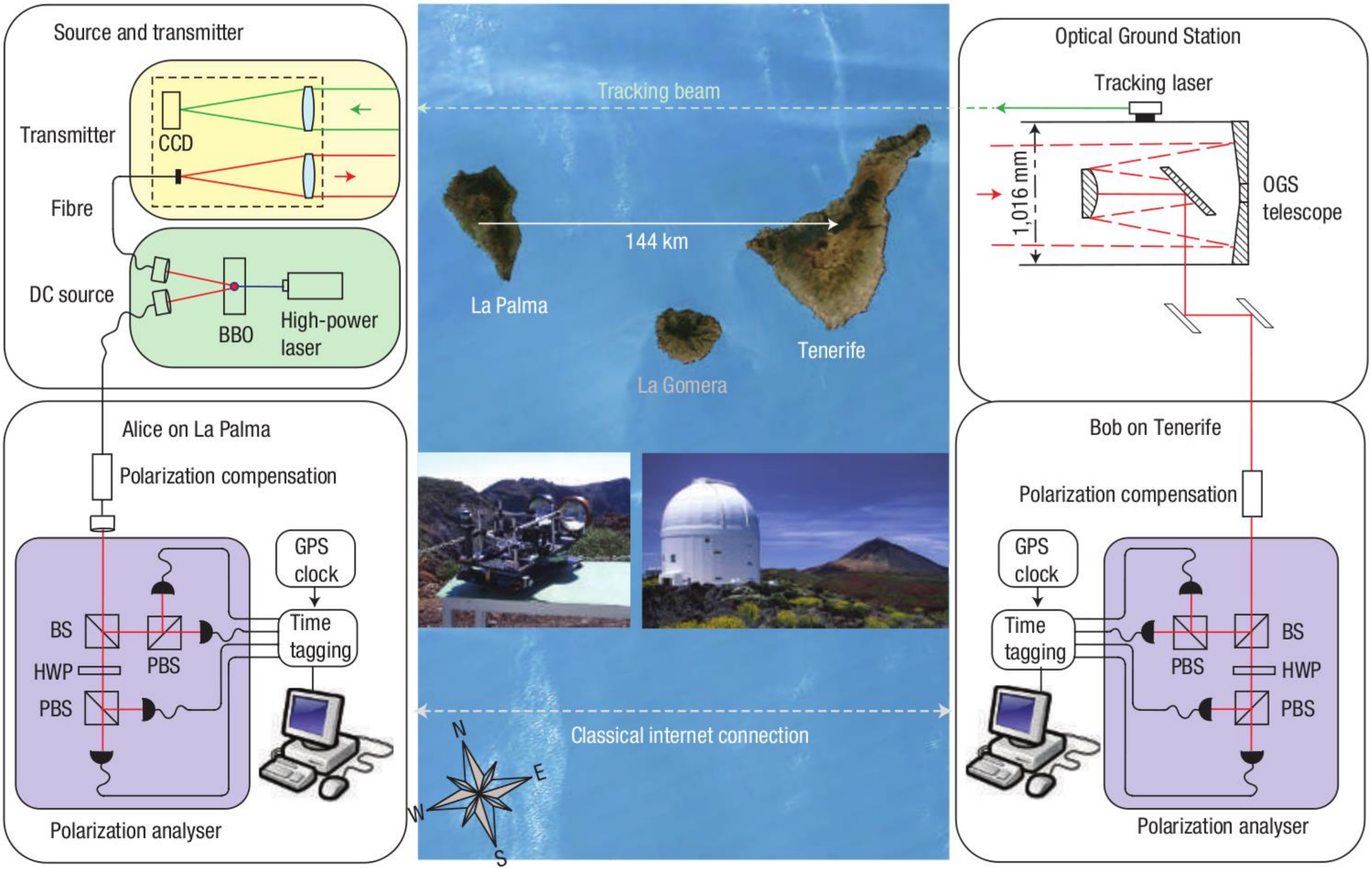
Alan Aspect
1947

~~LOCAL REALISM~~

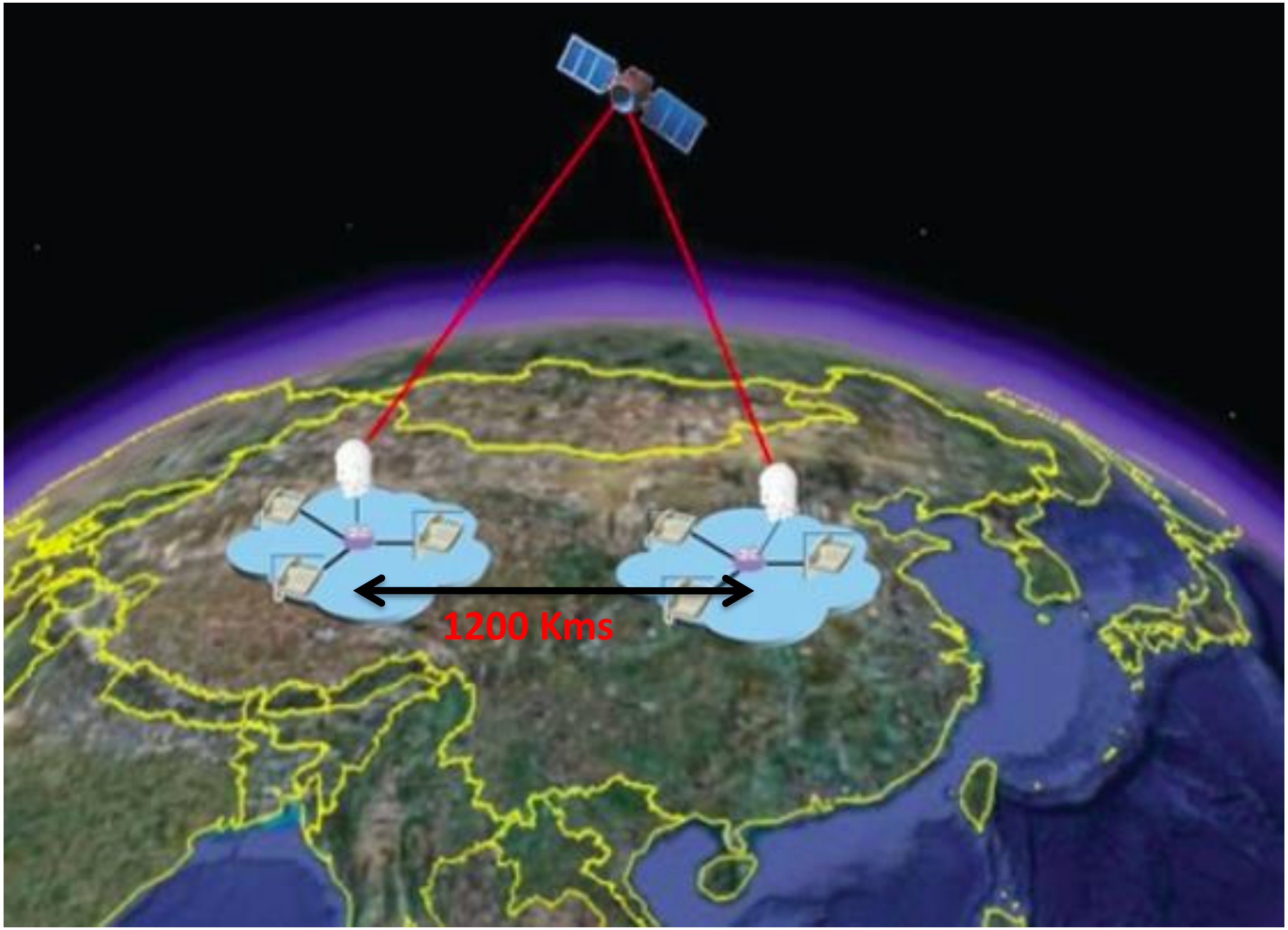
Bell experiment in Austria, Innsbruk (1998)

G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger,

Bell experiment in Canary islands (2007)



QESS (Quantum Entanglement at Space Scale) 2016-2018



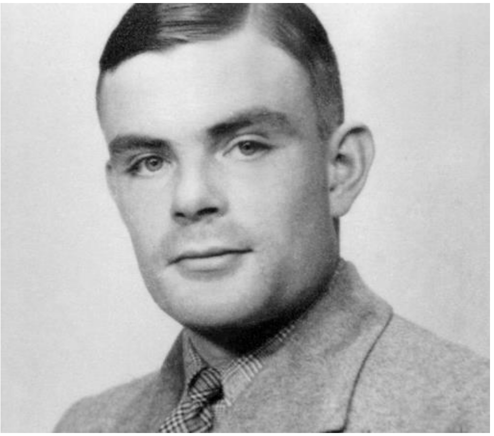
Joint Proyect China and Austria

Quantum Mechanics

Computer Sciences

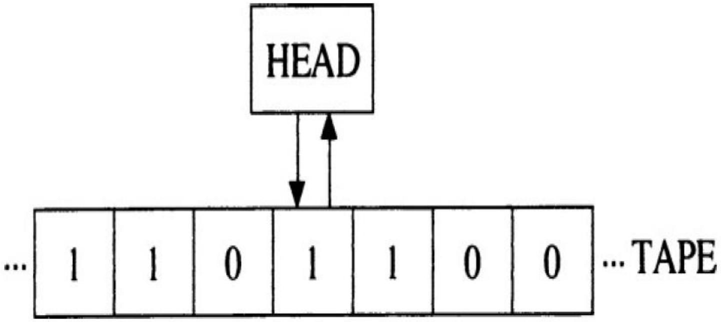
Quantum Computation
and
Quantum Information

Computer Sciences



Alan Turing (1914-1944)

Turing machine

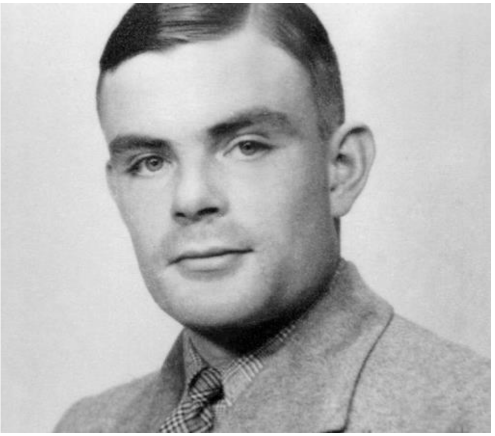


Program :

$Cunit$	$Tape$	$Cunit$	$Tape$	$Direction$
s_1	b	s_2	b	l
s_2	b	s_3	b	l
s_2	1	s_2	1	l
s_3	b	H	b	$-$
s_3	1	s_4	b	r
s_4	b	s_2	1	l

$$b\,1 \overset{n_1}{\cdots} 1\, b\, b\, 1 \overset{n_2}{\cdots} 1 \overset{s_1\downarrow}{b} \rightarrow b\,1 \overset{n_1+n_2}{\cdots} 1\, b \rightarrow \text{Halt}$$

Alonzo Church (1903-1995)



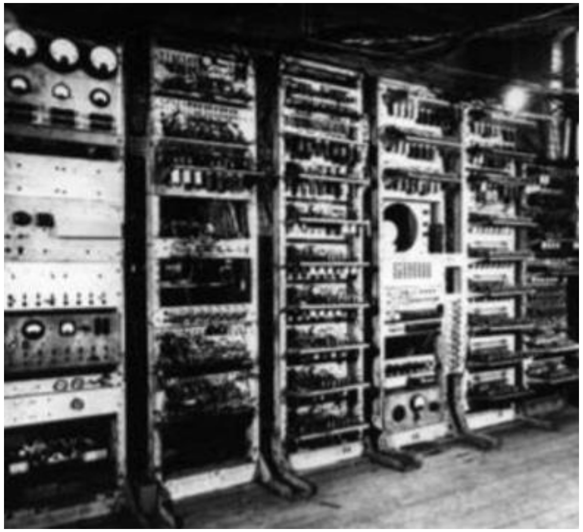
Alan Turing (1914-1944)

The Chuch-Turing thesis (1936)

Any algorithmic process can be simulated efficiently using a Turing machine

Turing, computers and crytography

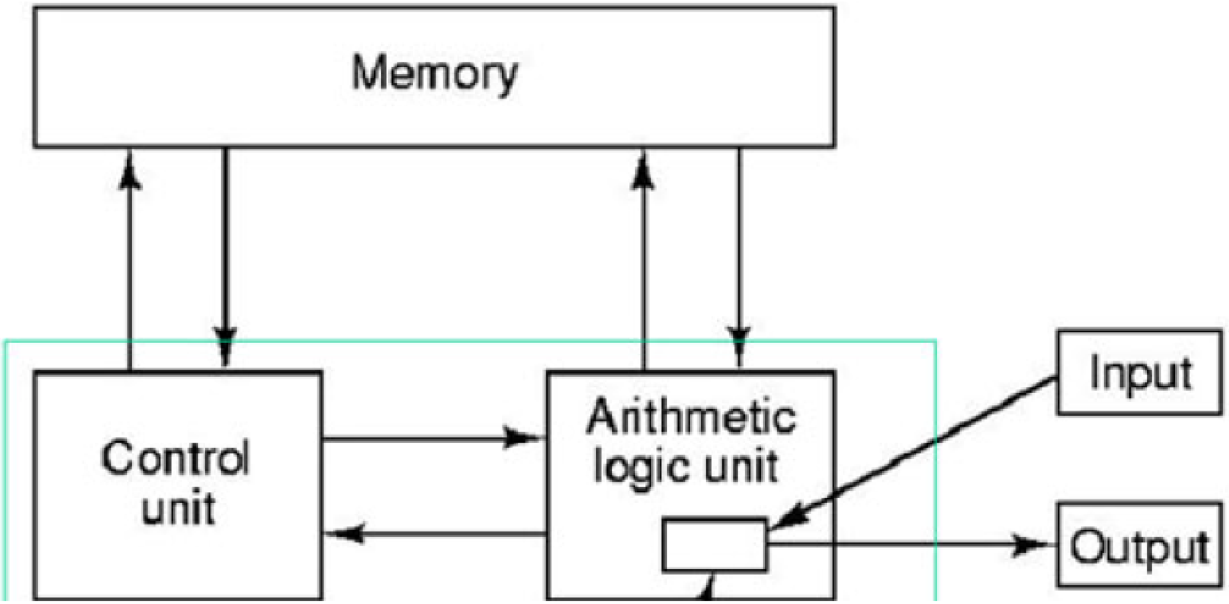
Enigma machine
Museo scienza e tecnologia Milano,



Electronic computer at the Manchester university 1950

John von Neumann
1903-1957

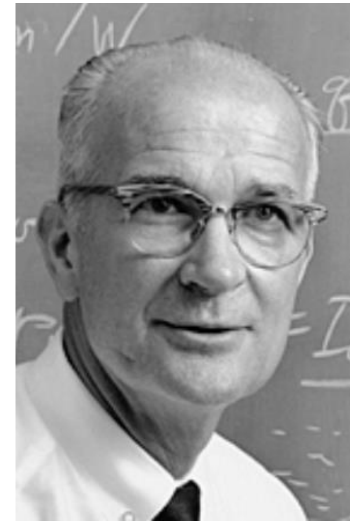
The architect of the computers



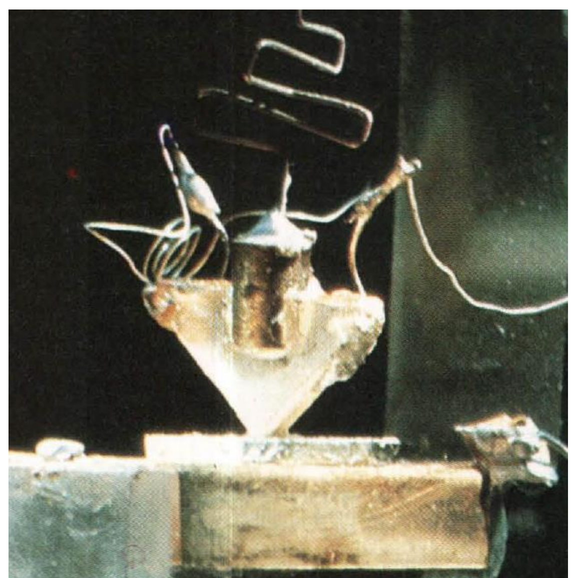
The first transistor (1947)

John Bardeen
1908-1991

Walter Brattain
1902-1987

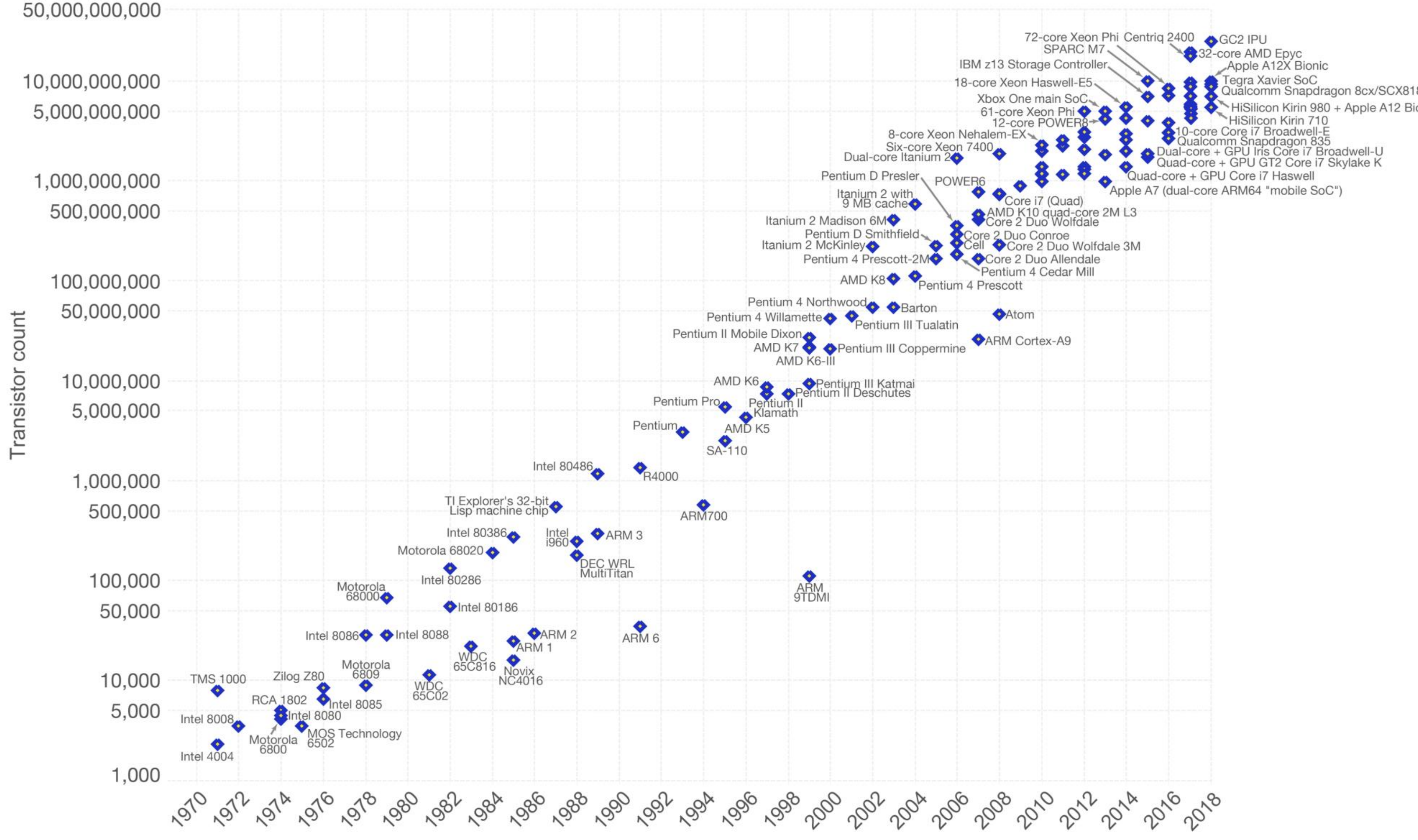


William Schockley
1902-1987



Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

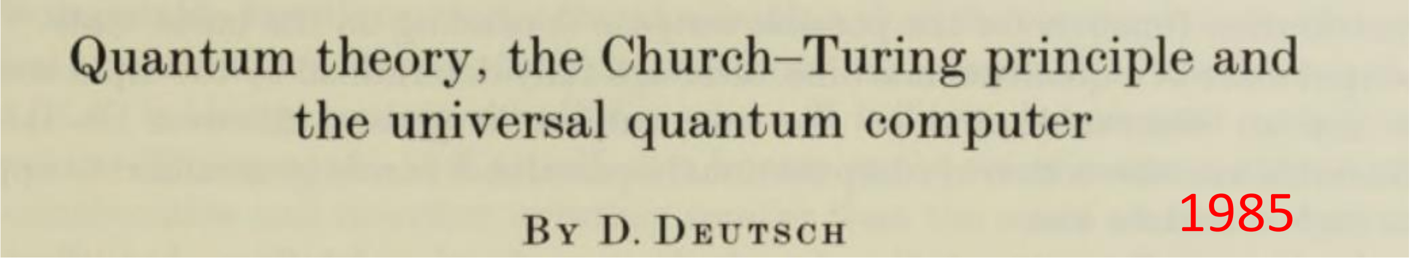
Richard Feynman
1918-1988

Simulating Physics with Computers

Richard P. Feynman 1982

Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

David Deutsch 1953



Quantum theory, the Church–Turing principle and the universal quantum computer

By D. Deutsch

1985

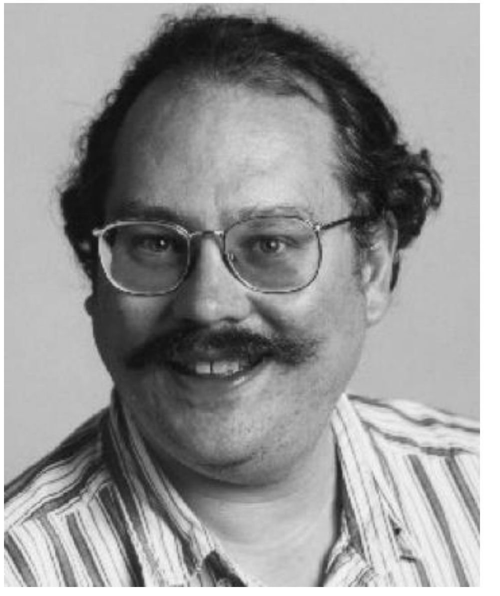
Proposed a quantum generalization of the Turing machines

= Quantum Computer

Title:Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

Authors:Peter W. Shor (AT&T Research)

arXiv:quant-ph/9508027



Peter Shor 1959

Computational time Prime factorization

N: integer, n = log N: number of digits

Best classical algorithm: $O\left(e^{1.9\, n^{1/3} (\log n)^{2/3}}\right)$

↓

Exponential speedup

Shor's algorithm: $O(n^2 \log n \log \log n)$

Lov Grover 1961

A fast quantum mechanical algorithm for database search

arXiv:quant-ph/9605043

Searching an item in a list of N data takes classicaly order N steps

In a quantum computer it takes order $\sqrt{N}$

quadratic speedup $N \rightarrow \sqrt{N}$

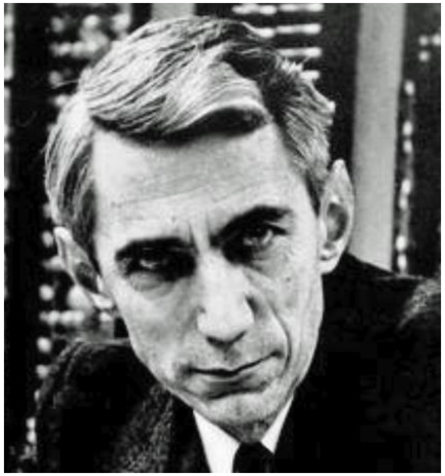
Quantum Mechanics

Computer Sciences

Quantum Computation and Quantum Information

Information Theory

Information theory

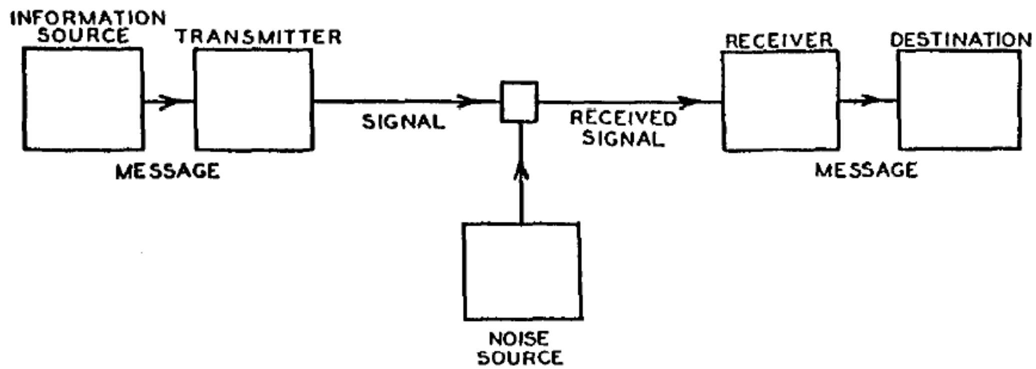


Claude Shannon
1916-2001

A Mathematical Theory of Communication

By C. E. SHANNON

Published in THE BELL SYSTEM TECHNICAL JOURNAL **1948**



Capacity of a communication channel

$$C = \lim_{T \to \infty} \frac{\log N(T)}{T}$$

Measure of information: Entropy

$$H = -K \sum_{i=1}^{n} p_i \log p_i$$

Noiseless channel coding theorem -> optimal resources to store information

Noisy channel coding theorem -> amount of information that can be reliable transmitted

Error correcting codes - > to protect information transmitted from the noise

The Minivac 601, a digital computer trainer designed by Shannon.

1962

Benjamin Schumacher

Quantum coding 1995

Quantum version of Shannon theory

Shannon entropy -> von Neumann entropy

Noiseless coding theorem -> quantum noiseless coding theorem

Introduced the terminology “quantum bit = qubit”

Benjamin Schumacher

Quantum coding 1995

Quantum version of Shannon theory

Shannon entropy -> von Neumann entropy

Noiseless coding theorem -> quantum noiseless coding theorem

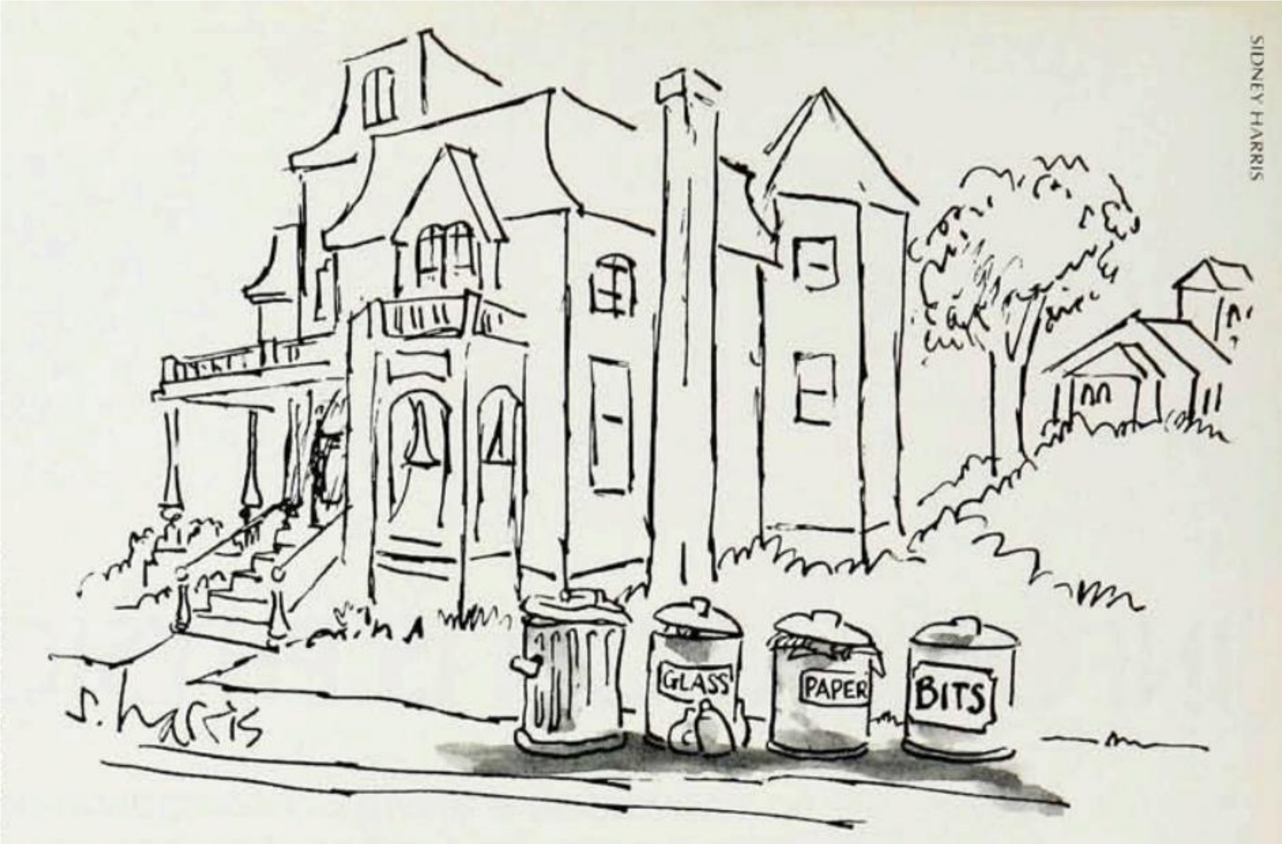
Introduced the terminology “quantum bit = qubit”

ACKNOWLEDGMENTS

The term “qubit” was coined in jest during one of the author’s many intriguing and valuable conversations with W. K. Wootters, and became the initial impetus for this work. The author is also grateful to C. H. Bennett and R. Jozsa for their helpful suggestions and for numerous words of encouragement.

Information is physical

Physics Today 44, 5, 23 (1991)



Rolf Landauer
1927-1999

Information is physical

Physics Today 44, 5, 23 (1991)

Rolf Landauer
1927-1999

Landauer principle

$$E = k_B T \ln 2$$

Cryptography

See talk "Introduction to Quantum Communication" by Vicente Martin (UPM), Thursday 2nd Sept

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

1984

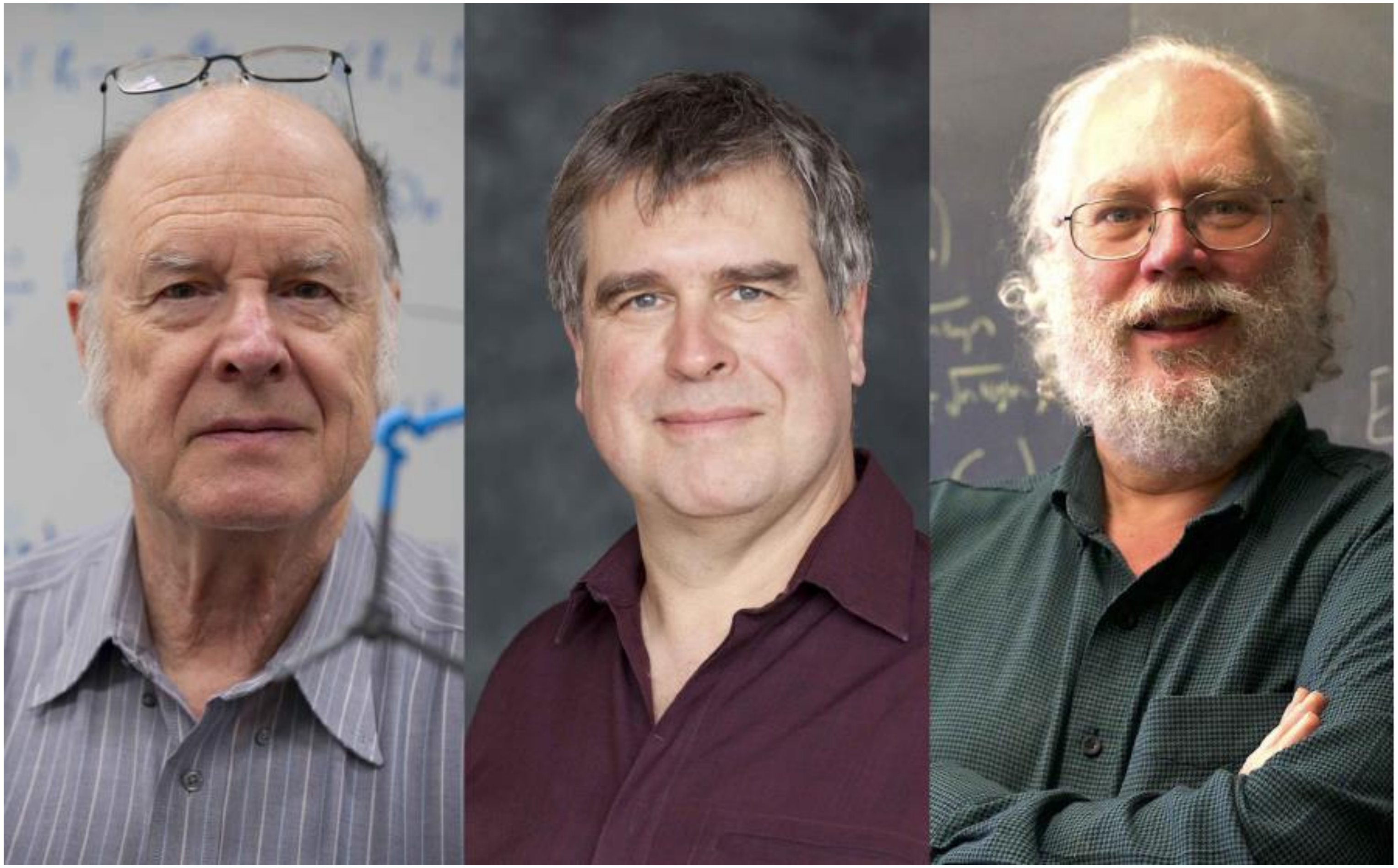
Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

Charles Bennet 1943

Gilles Brassard 1955

The BBVA prize Frontiers of Knowledge Award in Basic Sciences
to Charles Bennett, Gilles Brassard, and Peter Shor in 2019
for their respective roles in the development of quantum computing and cryptography



***The 19th century was the era of steam power,
the 20th century was the era of information,
and the 21st century will go down in history as
the quantum age, the age in which quantum
technologies dominate all the changes occurring
in society, in a way we cannot yet foresee."***

G. Brassard,
2019

Principles of Quantum Mechanics in a nutshell

Information ψ

Measurement

Composite systems

Evolution $U\psi$

The qubit

qubit = a quantum state of a two level system

Example of a qubit : spin ½ particle

$$|0\rangle = |\uparrow\rangle$$

$$|1 = |\downarrow\rangle$$

computational basis $|0\rangle\,,|1\rangle$

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

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = 0$$

Superposition principle

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle, \qquad a, b \in \mathbb{C}$$

$$\langle\psi|\psi\rangle = 1 \;\rightarrow\; |a|^2 + |b|^2 = 1 \qquad\qquad e^{i\alpha}|\psi\rangle\,,\, \alpha \,\epsilon\, \mathbb{R}$$ same state

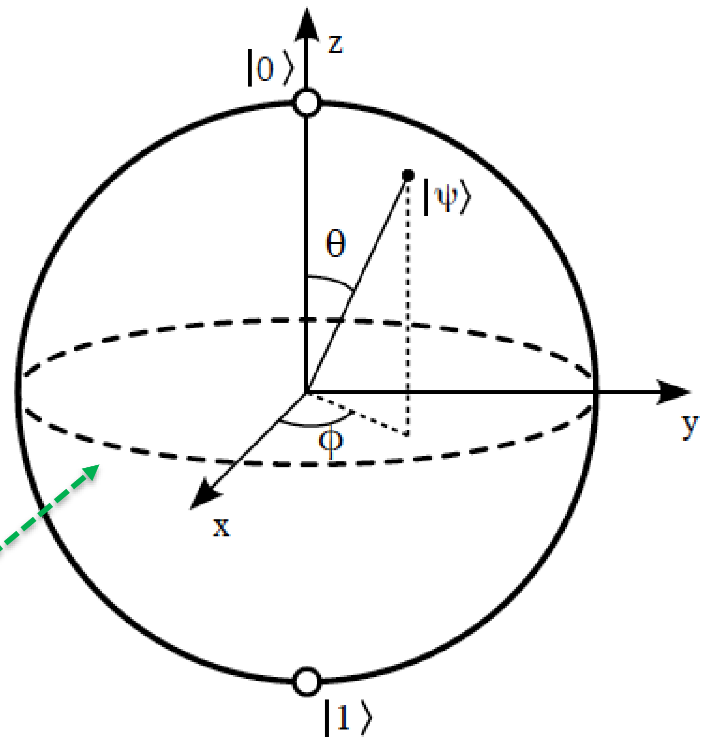
Standard parametrization

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \; e^{i\,\phi}\sin\frac{\theta}{2}|1\rangle \;= \begin{pmatrix} cos\,\frac{\theta}{2} \\ e^{i\phi}\; sin\,\frac{\theta}{2} \end{pmatrix}$$

$$\theta \;\in\; [0, \pi] \qquad\qquad \phi \;\in [0, 2\pi)$$

Geometric representation: Bloch sphere

θ : polar angle ϕ : azimuthal angle

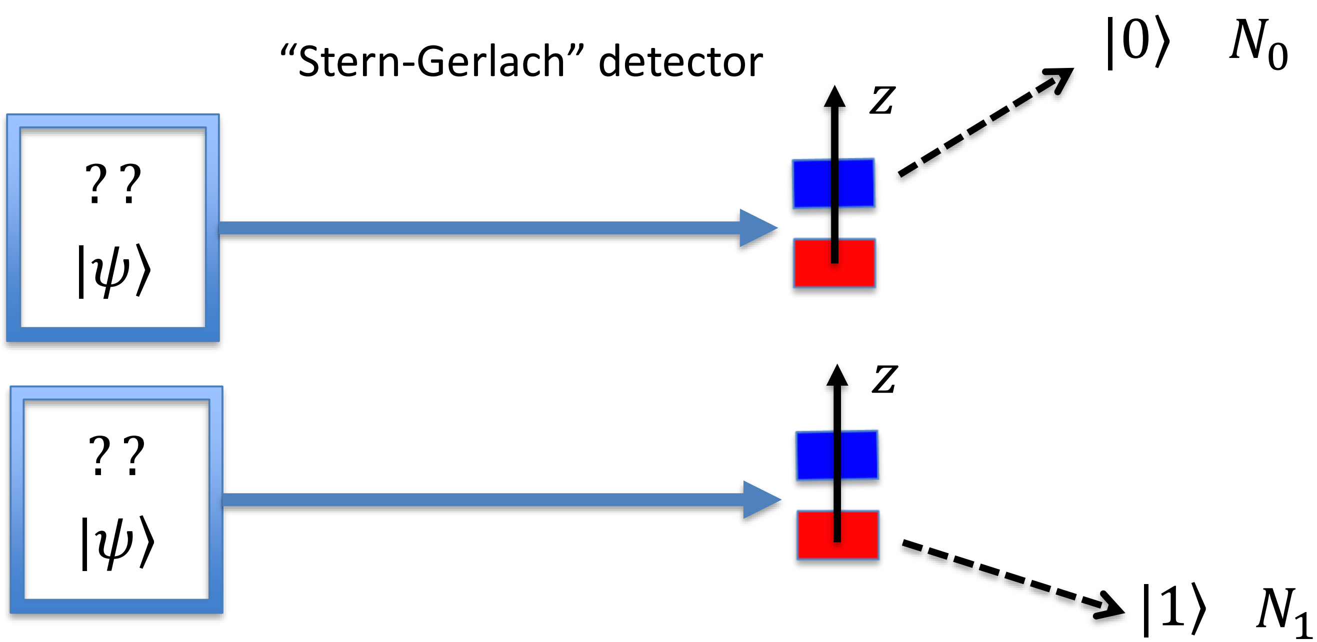


$$\frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}$$

Pure state of a qubit ⟺ Point on the Bloch sphere

How to compute the angles θ, ϕ ?

Prepare N times an unknown state in the Lab



$$N = N_0 + N_1$$

Probability of measuring $|0\rangle$ $$p_0 = \frac{N_0}{N_0 + N_1}$$

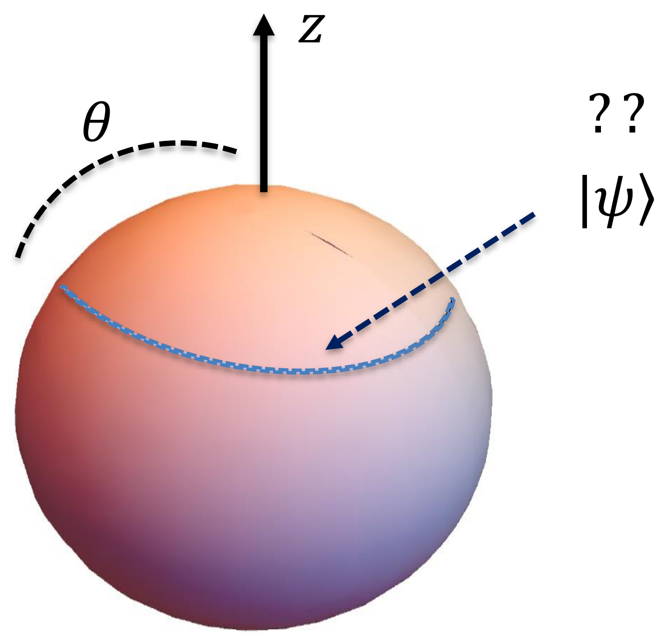
Probability of measuring $|1\rangle$ $$p_1 = \frac{N_1}{N_0 + N_1}$$

$$p_0 + p_1 = 1$$

Quantum Mechanical prediction

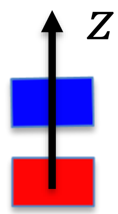
$$p_0 = |\langle 0|\psi\rangle|^2 = cos^2\frac{\theta}{2} \qquad p_1 = |\langle 1|\psi\rangle|^2 = sin^2\frac{\theta}{2}$$

Error $\propto 1/\sqrt{N}$



z
θ
??
$|\psi\rangle$

Stern-Gerlach detector



Observable

$$\sigma^z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Expectation value

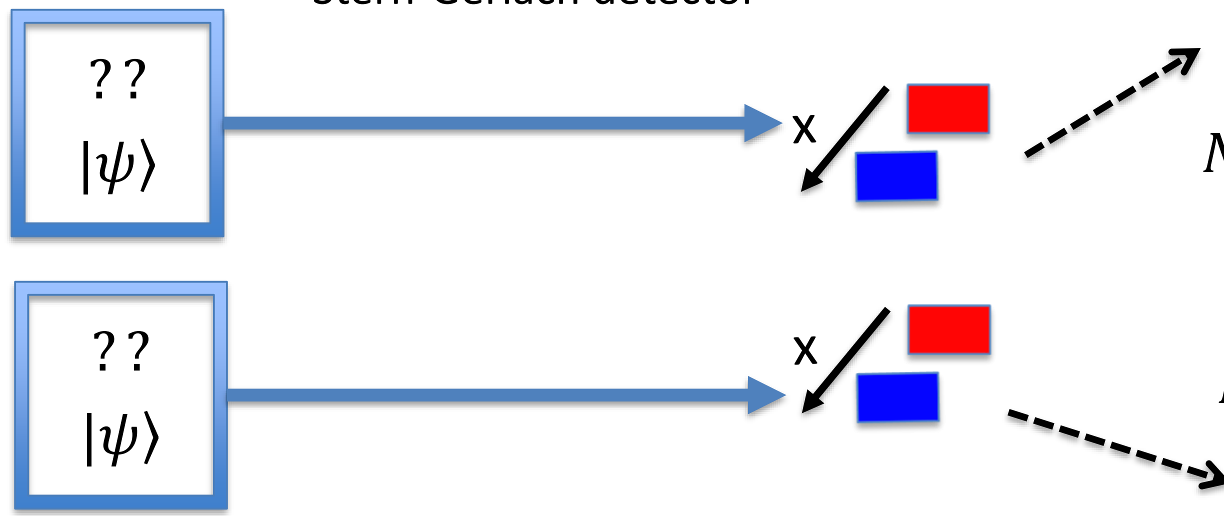
$$\langle \sigma^z \rangle = \ p_0 \ - \ p_1$$

QM $$\langle \sigma^z \rangle = \langle \psi | \sigma^z | \psi \rangle = cos^2 \frac{\theta}{2} - sin^2 \frac{\theta}{2} = \cos\theta$$

What about ϕ ?

Stern-Gerlach detector

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

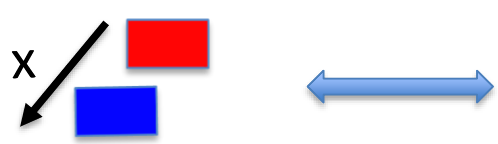


$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$N = N_+ + N_-$$

Stern-Gerlach detector

Observable



$$\sigma^x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Probability of measuring $|+\rangle$ $$p_+ = \frac{N_+}{N_+ + N_-}$$

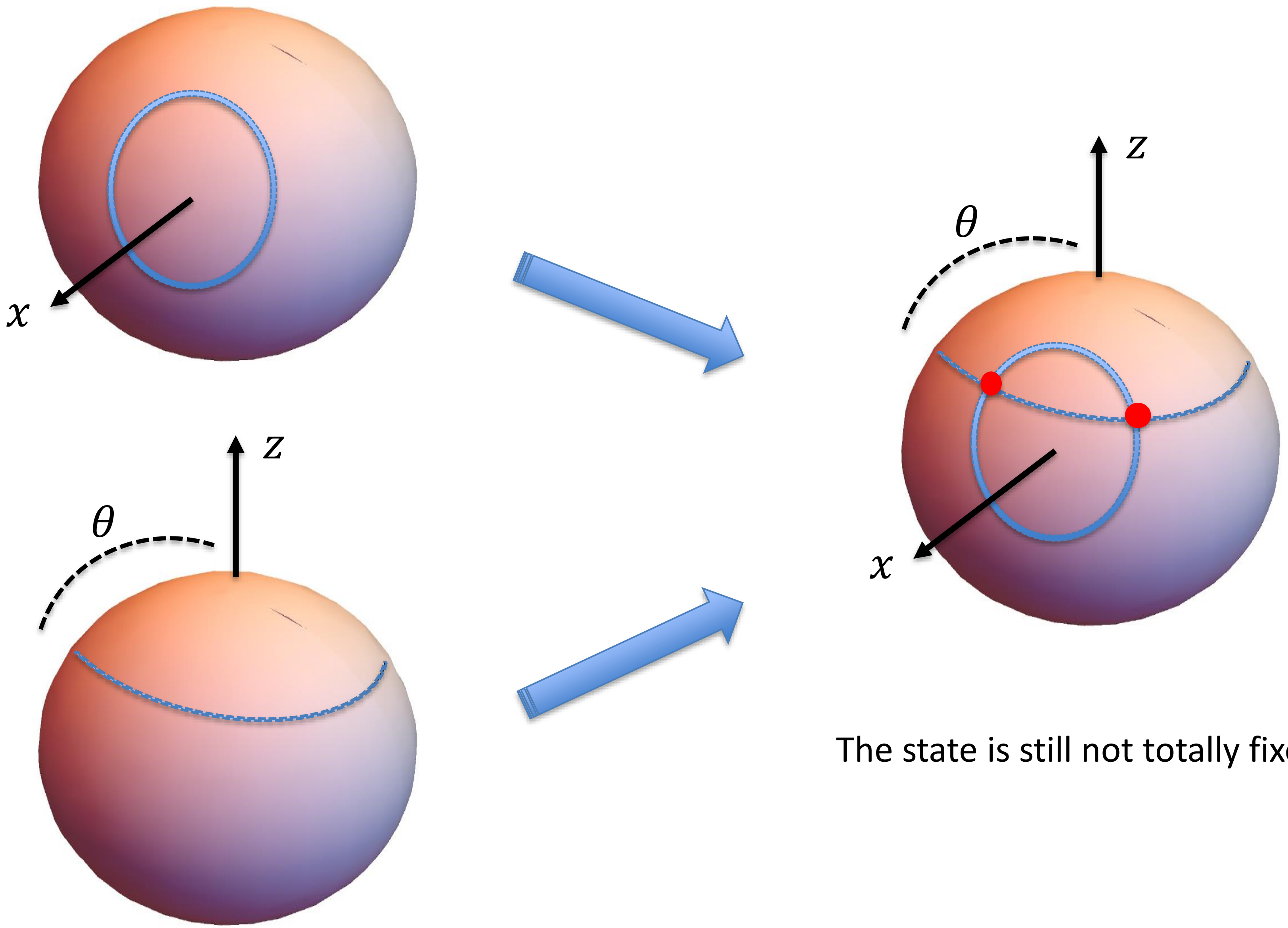
Probability of measuring $|-\rangle$ $$p_- = \frac{N_-}{N_+ + N_-}$$

Quantum Mechanical prediction

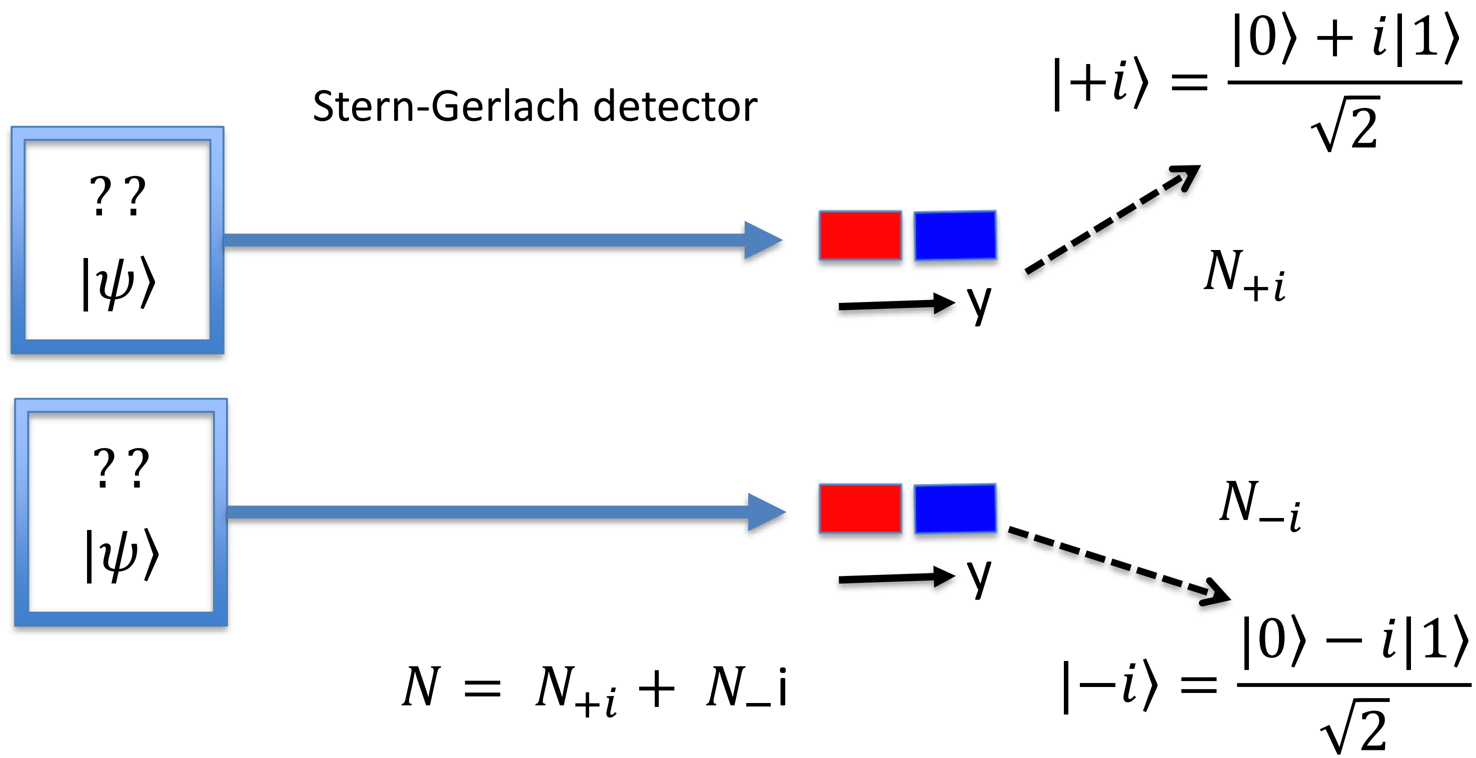
$$p_+ = |\langle + | \psi \rangle|^2 = \frac{1 + \sin\theta \cos\phi}{2} \qquad p_- = |\langle - | \psi \rangle|^2 = \frac{1 - \sin\theta \cos\phi}{2}$$

$$\langle \sigma^x \rangle = p_+ - p_-$$

QM $$\langle \sigma^x \rangle = \langle \psi | \sigma^x | \psi \rangle = sin\,\theta \cos\phi$$

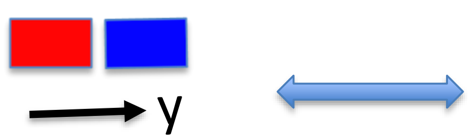


The state is still not totally fixed



Stern-Gerlach detector

Observable



$$\sigma^y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Probability of measuring $|+i\rangle$ $\qquad$ $$p_{+i} = \frac{N_{+i}}{N_{+i} + N_{-i}}$$

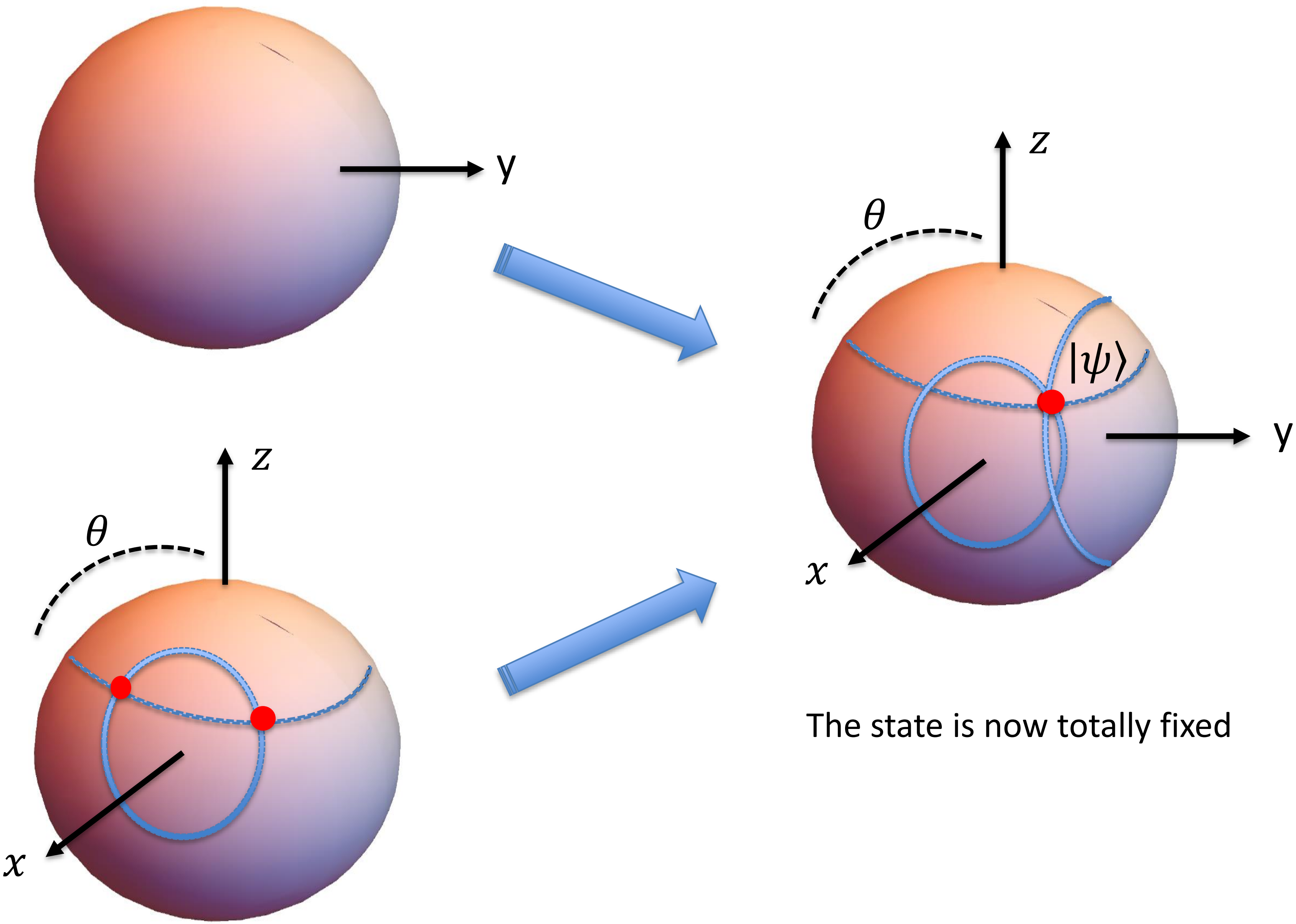
Probability of measuring $|-\rangle$ $\qquad$ $$p_{-i} = \frac{N_{-i}}{N_{+i} + N_{-i}}$$

Quantum Mechanical prediction

$$p_{+i} = |\langle +i|\psi\rangle|^2 = \frac{1 + \sin\theta\sin\phi}{2} \qquad p_{-i} = |\langle -i|\psi\rangle|^2 = \frac{1 - \sin\theta\sin\phi}{2}$$

$$\langle \sigma^y \rangle = p_{+i} - p_{-i}$$

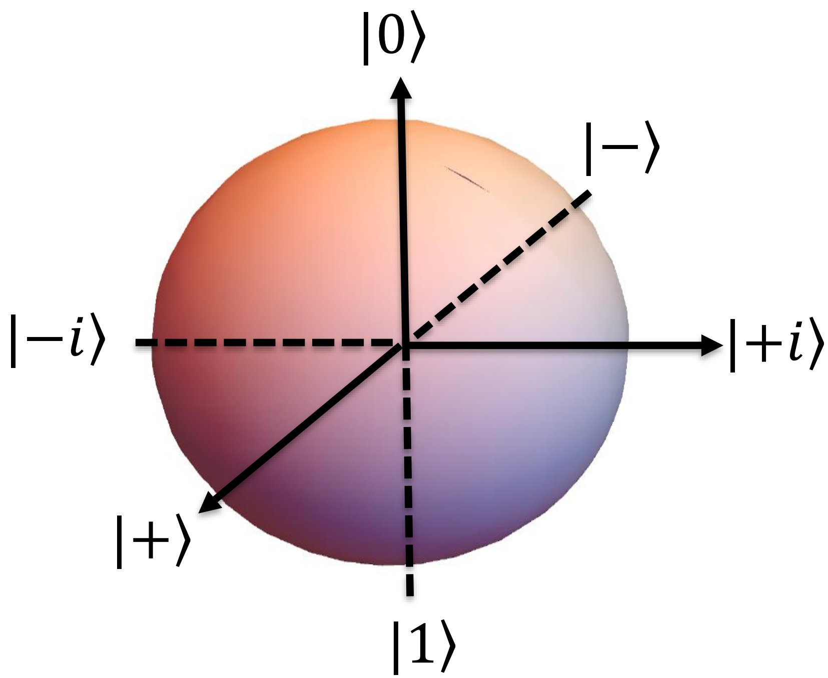
QM $\quad$ $$\langle \sigma^y \rangle = \langle \psi|\sigma^y|\psi\rangle = sin\,\theta\sin\phi$$



The state is now totally fixed

$$\begin{cases} \langle \sigma^x \rangle = \cos\phi \sin\ \theta = x \\ \langle \sigma^y \rangle = \sin\phi \sin\ \theta = y \\ \langle \sigma^z \rangle = \cos\theta = z \end{cases}$$

$$|\psi\rangle = \begin{pmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x + i\, y}{\sqrt{2(1+z)}} \end{pmatrix}$$



Density matrix

Classical Mechanics

A “pure” state of a 1D particle is given by the point in the phase space (q,p)

A “mixed” state is given by a probability density $\rho(q,p)$

Expectation values of an observable $\mathcal{O}(q,p)$ is given by $\langle \mathcal{O} \rangle = \int dq\, dp\, \rho(q,p)\, \mathcal{O}\,(q,p)$

Density matrix

Classical Mechanics

A "pure" state of a 1D particle is given by the point in the phase space (q,p)

A "mixed" state is given by a probability density $\rho(q,p)$

Expectation values of an observable $\mathcal{O}(q,p)$ is given by $\langle\mathcal{O}\rangle = \int dq\, dp\, \rho(q,p)\, \mathcal{O}\,(q,p)$

Quantum Mechanics

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} cos^2\frac{\theta}{2} & e^{-i\phi}\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ e^{i\phi}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & sin^2\frac{\theta}{2} \end{pmatrix}$$

$$\langle O\rangle = Tr(\rho\, O)$$

$$tr\,\rho = 1$$

$$\rho^\dagger = \rho$$

$$\rho > 0$$

Mixed state

Ensemble of N pure states $|\psi_i\rangle$ with probabilities p_i

$$\rho = \sum_{i=1}^{N} p_i \, |\psi_i\rangle \, \langle\psi_i| \qquad 1 = \sum_{i=1}^{N} p_i$$

General state

$$\rho = \frac{1}{2} \begin{pmatrix} 1+z & x-i\,y \\ x+i\,y & 1-z \end{pmatrix} = \frac{1}{2}\,(1 + x\,\sigma^x + y\,\sigma^y + z\,\sigma^z)$$

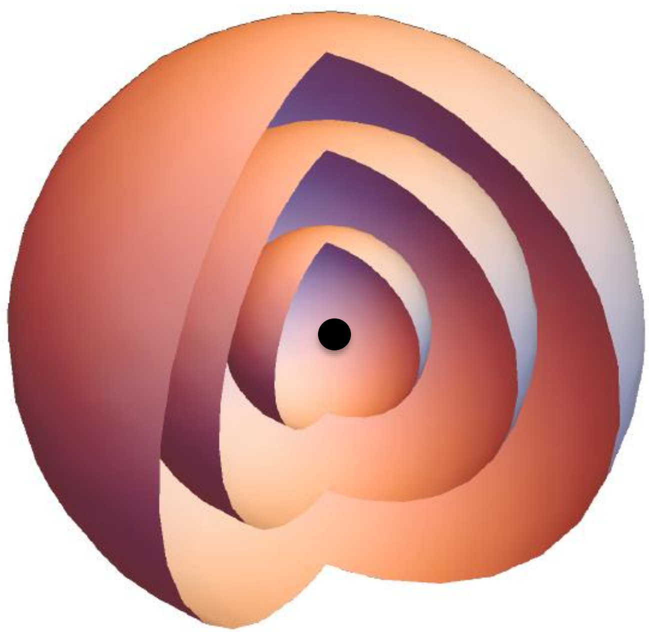
Eigenvalues $\dfrac{1+r}{2}, \dfrac{1-r}{2}$ $\qquad r = \sqrt{x^2 + \, y^2 + \, z^2}$

$$\rho > 0 \; \rightarrow 0 \; \leq r \; \leq 1$$

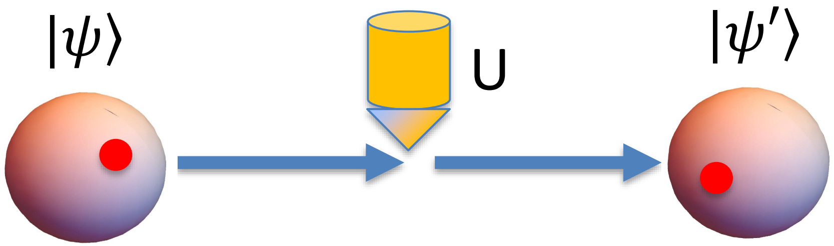
$$\langle\sigma^x\rangle = Tr(\rho\sigma^x) = x, \langle\sigma^y\rangle = Tr(\rho\sigma^y) = y, \langle\sigma^z\rangle = Tr(\rho\sigma^z) = z$$

Pure states:	$r = 1$	$\rho = \|\psi\rangle\langle\psi\|$
Mixed states:	$r < 1$	$\rho \neq \|\psi\rangle\langle\psi\|$
Maximally mixed state:	$r = 0$	$\rho = \frac{I}{2}$

Bloch ball



Single qubit gates



$$\mathrm{U}\,|\psi\rangle = |\psi'\rangle$$

$$\langle\psi'|\psi'\rangle = \langle\psi|\,U^{\dagger}\,U\,|\psi\rangle = \langle\psi|\psi\rangle$$

$$U^{\dagger}U = \mathbb{I}$$

U unitary matrix

Pauli gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Hadamard gate

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

S gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

T gate

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

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

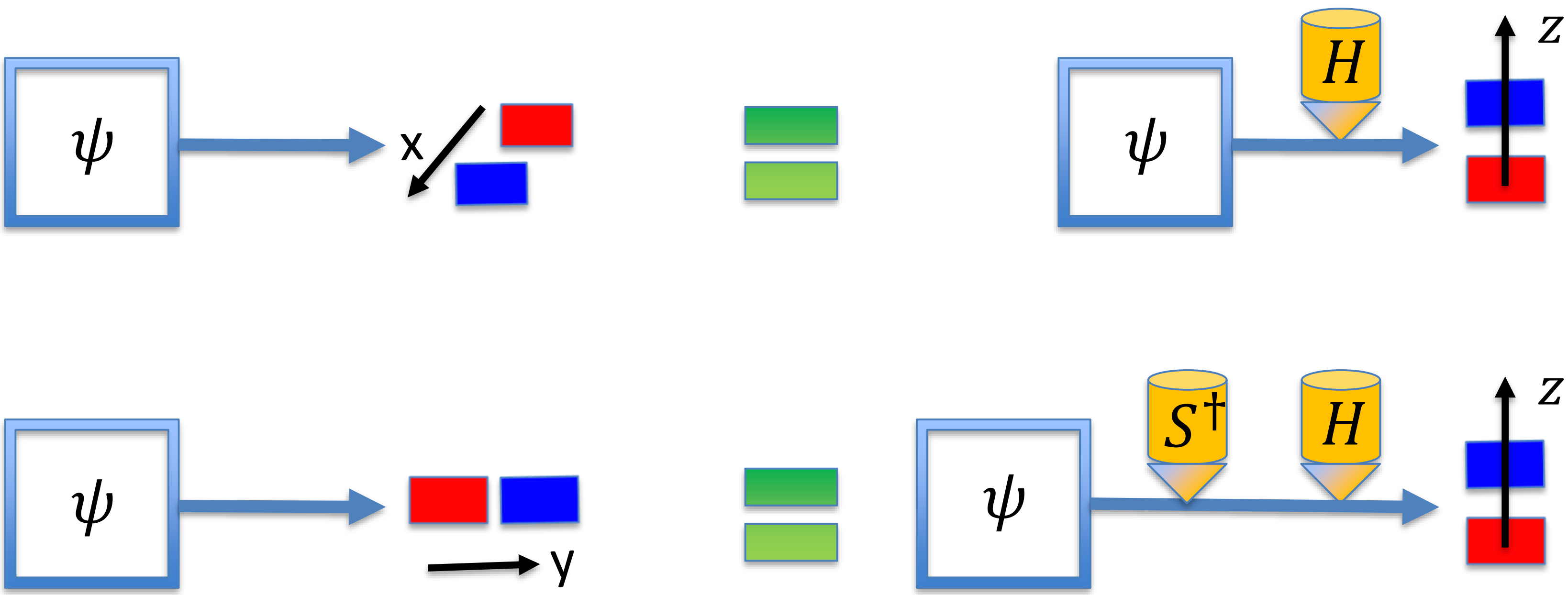
$$H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

Hadamard's magic

$$X = H\, Z\, H \qquad\qquad Y = S\, H\, Z\, H\, S^{\dagger}$$

$$\langle X \rangle_{\psi} = \langle \psi | X | \psi \rangle = \langle \psi | H\, Z\, H | \psi \rangle = \langle Z \rangle_{H\psi}$$

$$\langle Y \rangle_{\psi} = \langle \psi | Y | \psi \rangle = \langle \psi \big| S\, H\, Z\, H\, S^{\dagger} \big| \psi \rangle = \langle Z \rangle_{HS^{\dagger}\psi}$$

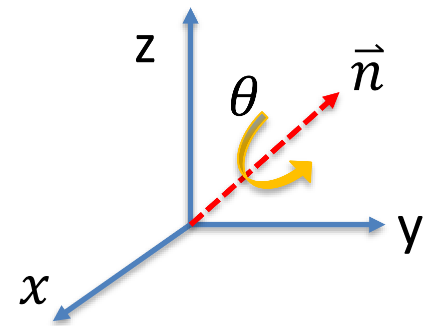


IBM tomography

General qubit gate

Qubit = spin ½ representation of the rotation group SU(2)

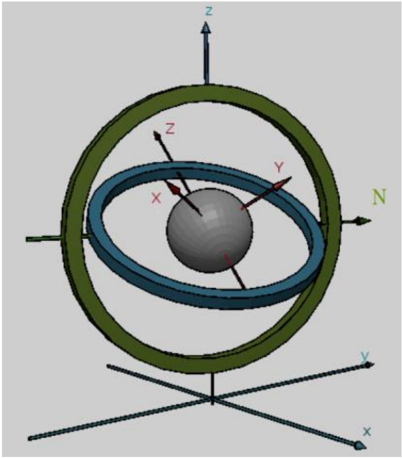
$$R_{\vec{n}}(\theta) = e^{-i\,\theta\vec{n}\cdot\vec{\sigma}/2}$$



$$U = e^{i\alpha} R_{\vec{n}}(\theta)$$

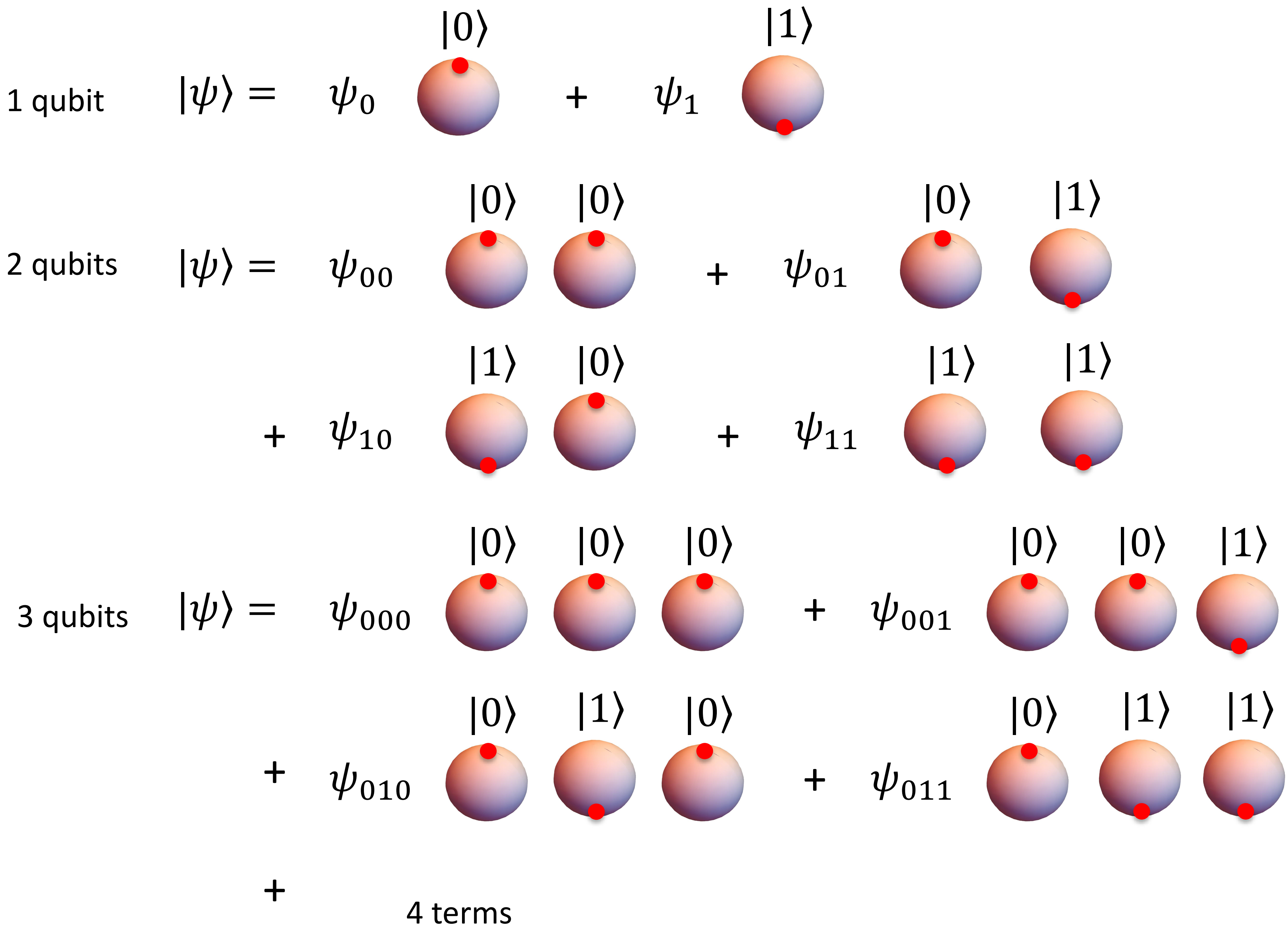
Euler's decomposition $U = e^{i\alpha} R_z(\beta)\, R_y(\gamma) R_z(\delta)$

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



gimbal set

Multiqubit states



State vectors

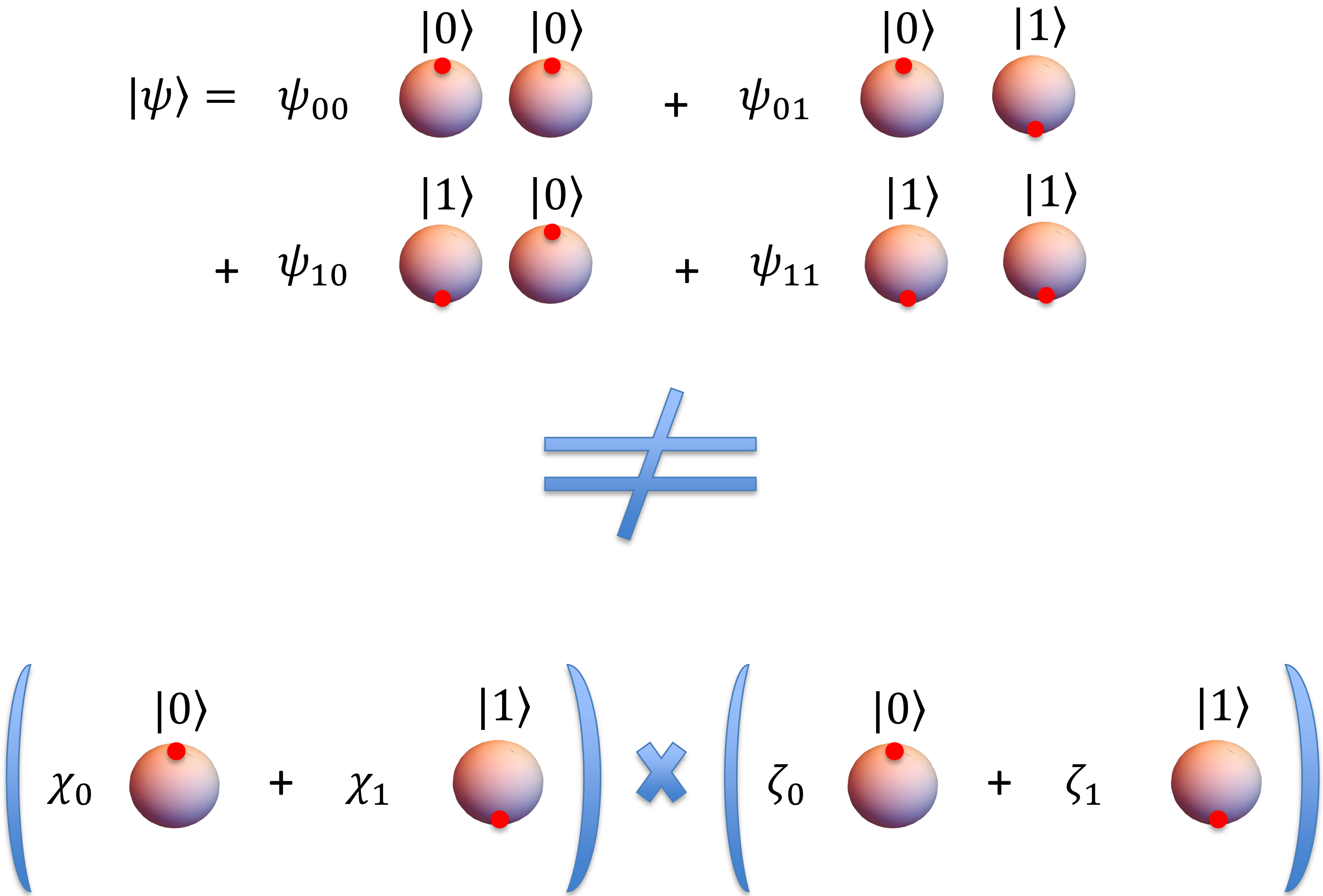
1 qubit $|\psi\rangle = \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix}$

2 qubits $|\psi\rangle = \begin{pmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{pmatrix}$

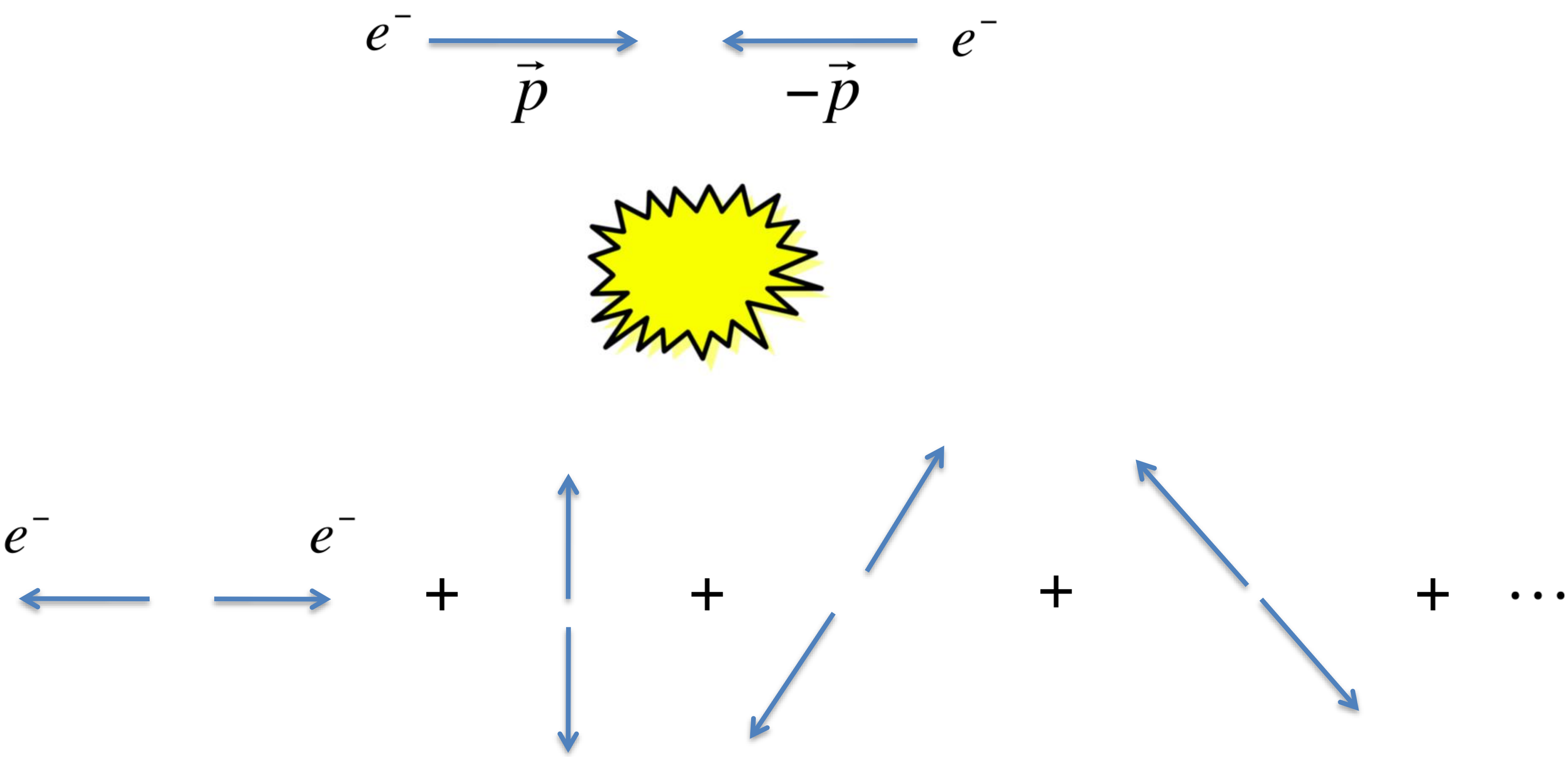
3 qubits $|\psi\rangle = \begin{pmatrix} \psi_{000} \\ \psi_{001} \\ \psi_{010} \\ \psi_{011} \\ \psi_{100} \\ \psi_{101} \\ \psi_{110} \\ \psi_{111} \end{pmatrix}$

n qubits $|\psi\rangle =$ vector with 2^n components

Entangled states



EPR state : Gedanken experiment



Linear superposition of two electrons with opposite momentum

How to create entanglement?

How to create entanglement?

Need a 2 qubit gate CNOT = Controlled NOT

How to create entanglement?

Need a 2 qubit gate   CNOT = Controlled NOT

control qbit   target qbit

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

How to create entanglement?

Need a 2 qubit gate   CNOT = Controlled NOT

control qbit   target qbit

$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |11\rangle \\
|11\rangle &\rightarrow |10\rangle
\end{aligned}
$$

$$|c, t\rangle \rightarrow |c, c \oplus t\rangle$$

$$c \oplus t = c + t \; mod \; 2$$

How to create entanglement?

Need a 2 qubit gate CNOT = Controlled NOT

control qbit → target qbit

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

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

$$|c,t\rangle \rightarrow |c, c \oplus t\rangle$$

$$c \oplus t = c + t \ mod\ 2$$

How to create entanglement?

Need a 2 qubit gate   CNOT = Controlled NOT

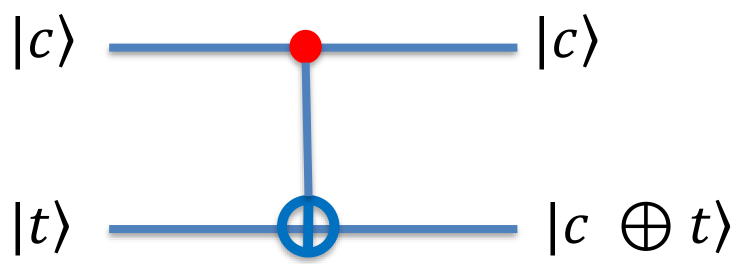
control qbit   target qbit

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

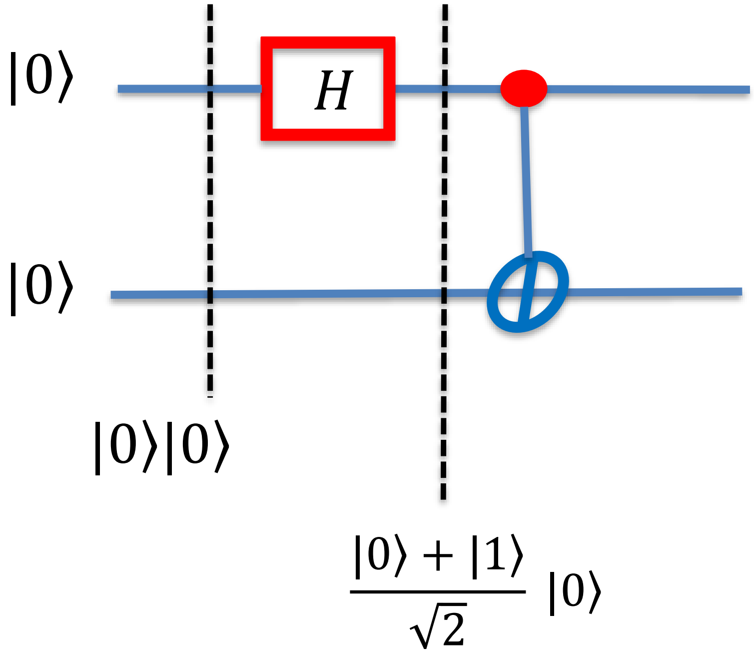
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|c, t\rangle \rightarrow |c, c \oplus t\rangle$$

$$c \oplus t = c + t \ mod\ 2$$

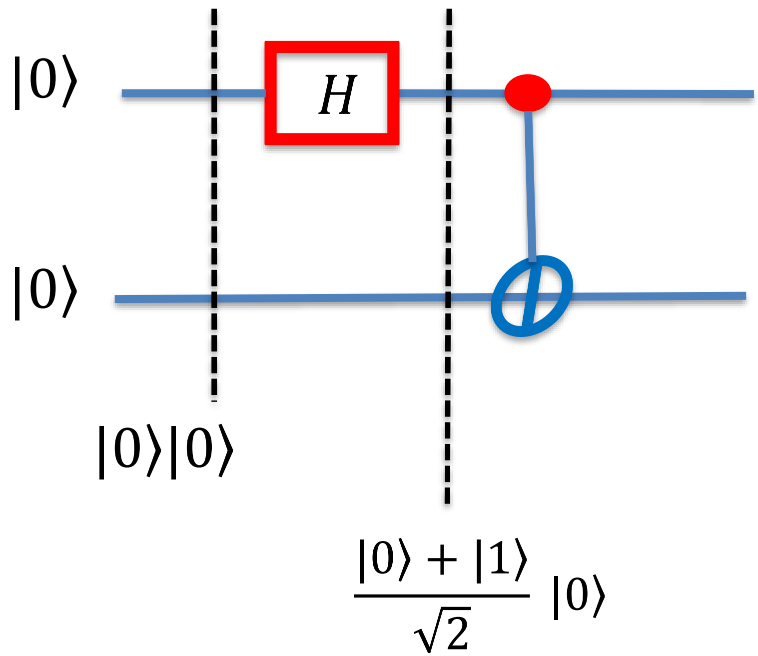


Creation of entanglement



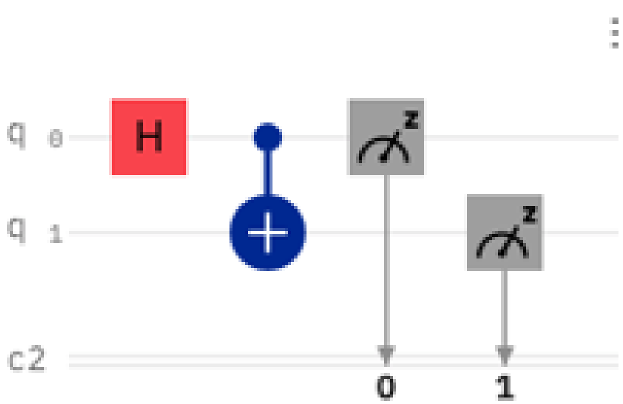
$$|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

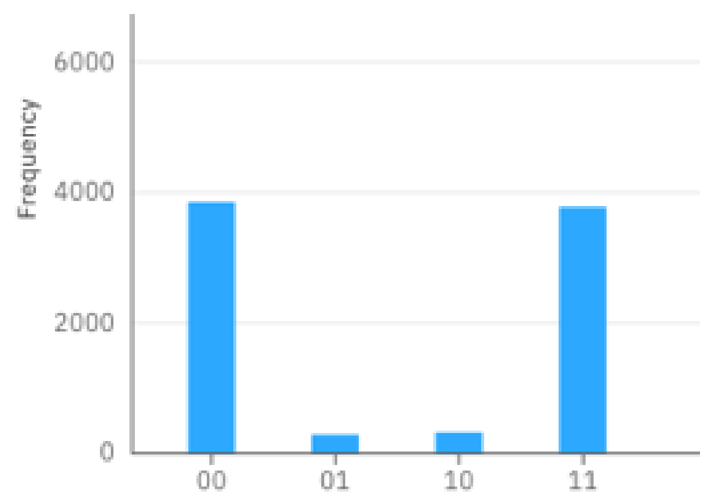
Creation of entanglement



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

IBMQ circuit





Bell basis for 2 qubit states

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

$$|\phi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

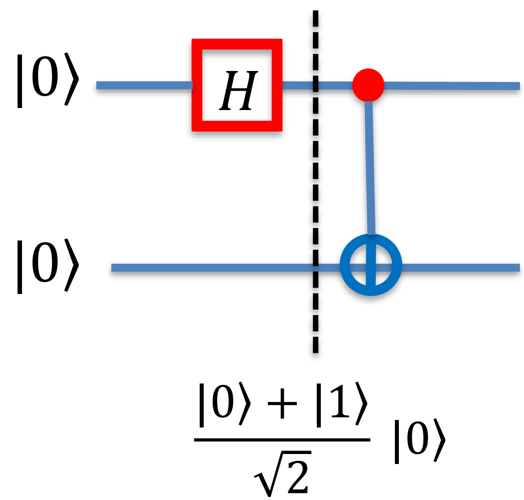
$$|\psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

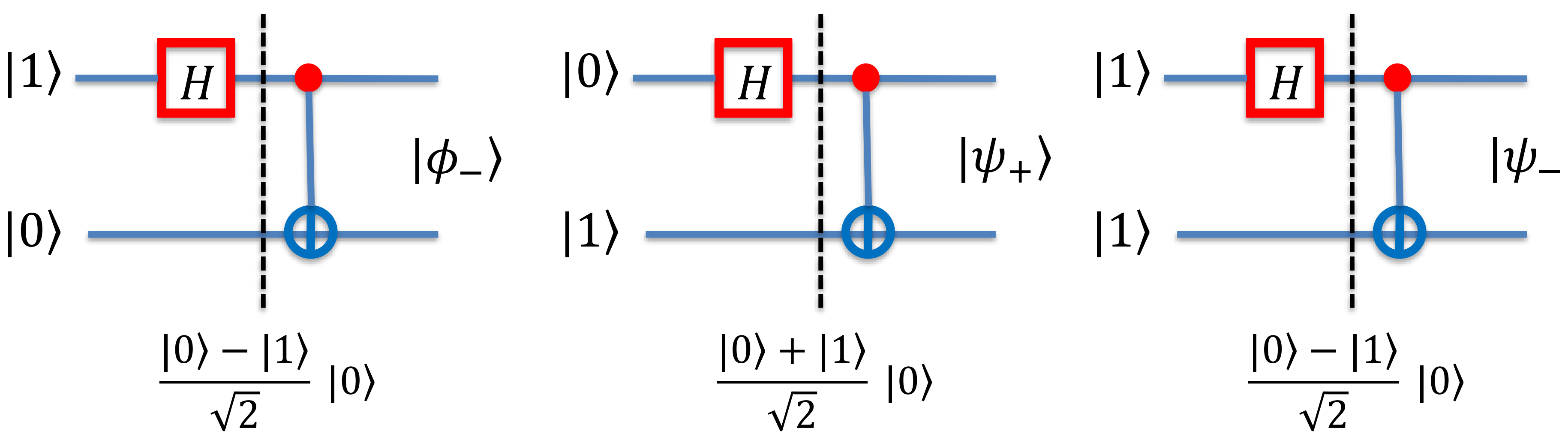
The qubits are maximally entangle for each of these states

Used in the teleportation protocol

Creation of entanglement

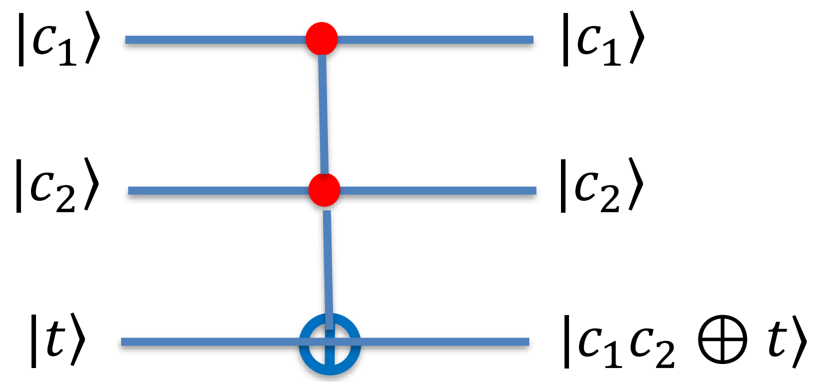


$$|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



Computational basis -> Bell basis

Toffoli gate = CCNOT



Universal classical gates

A finite set of gates that can be used to compute any function

Non reversible: AND, OR, NOT

Reversible: + Toffoli

Universal quantum gates

A finite set of quantum gates that can approximate any unitary operation to arbitrary precision

$\{ H, S, T, CNOT \}$ $\{ H, S, CNOT, TOFFOLI \}$

Deutsch's algorithm (1985)

The problem: given a boolean function $f(x)$ determine if it is constant or balanced

$$x \in \{0,1\}, \qquad f(x) \in \{0,1\}$$

There are 4 functions of this type

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Constant function: $f(0) = f(1)$

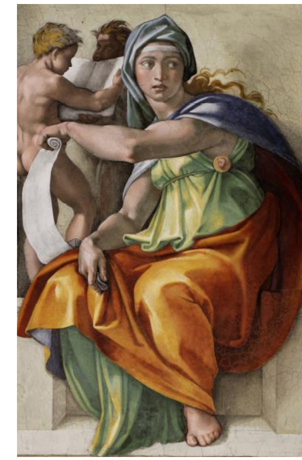
$f_0\,, f_3$

Balanced function: $f(0) \neq f(1)$

$f_1\,, f_2$

Given an unknown function to determine its character we have to compute

$$f(0) \quad \text{and} \quad f(1)$$

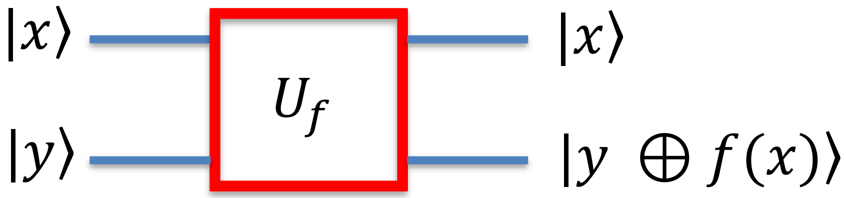


This is refereed to as “calling TWICE an oracle”

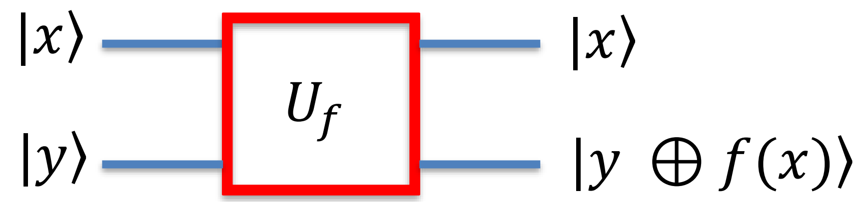
Question: Can one call only ONCE the oracle ?

Answer: YES using quantum parallelism and interference

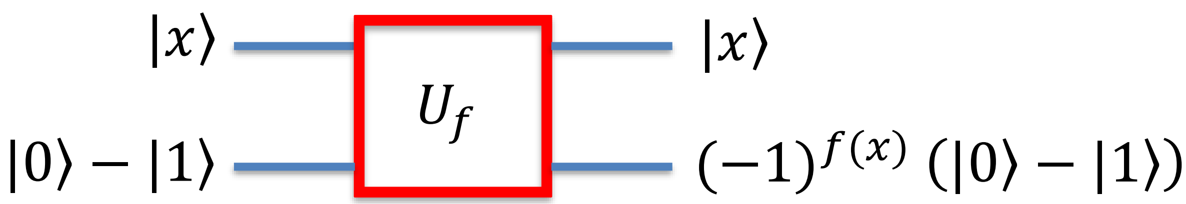
Quantum oracle



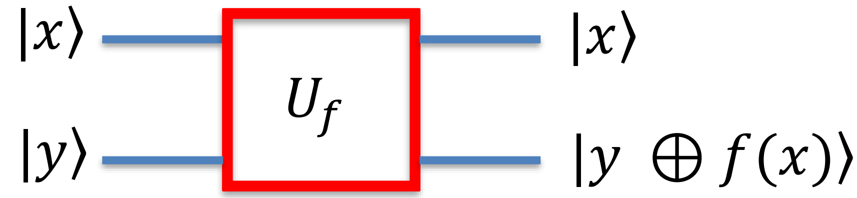
Quantum oracle



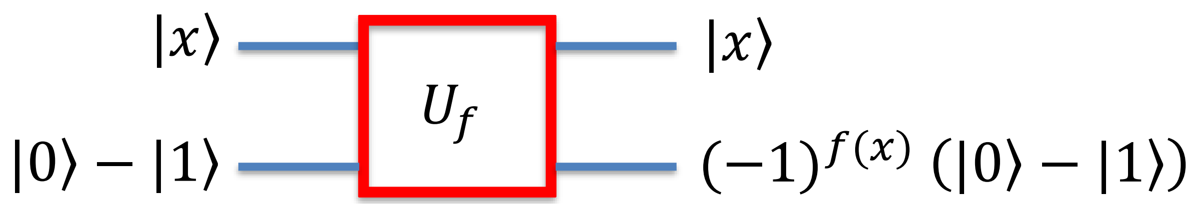
Step 1: call to the oracle



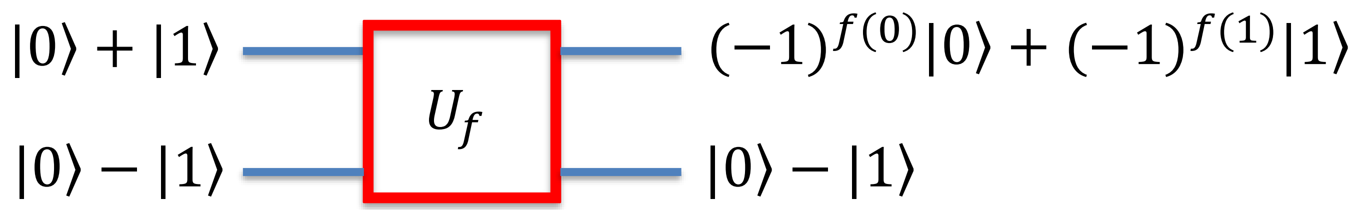
Quantum oracle



Step 1: call to the oracle

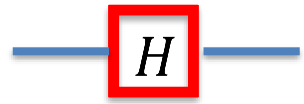


Step 2: interference of the answers



Step 3: quantum data mining

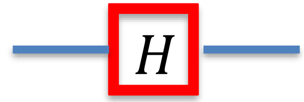
$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$



$$((-1)^{f(0)}+(-1)^{f(1)})|0\rangle$$
$$+$$
$$((-1)^{f(0)}-(-1)^{f(1)})|1\rangle$$

Step 3: quantum data mining

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$



$$\left((-1)^{f(0)}+(-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)}-(-1)^{f(1)}\right)|1\rangle$$

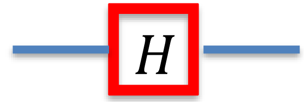
Step 4: getting the answer

If $f(0) = f(1)$ → $|0\rangle$

If $f(0) \neq f(1)$ → $|1\rangle$

Step 3: quantum data mining

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$



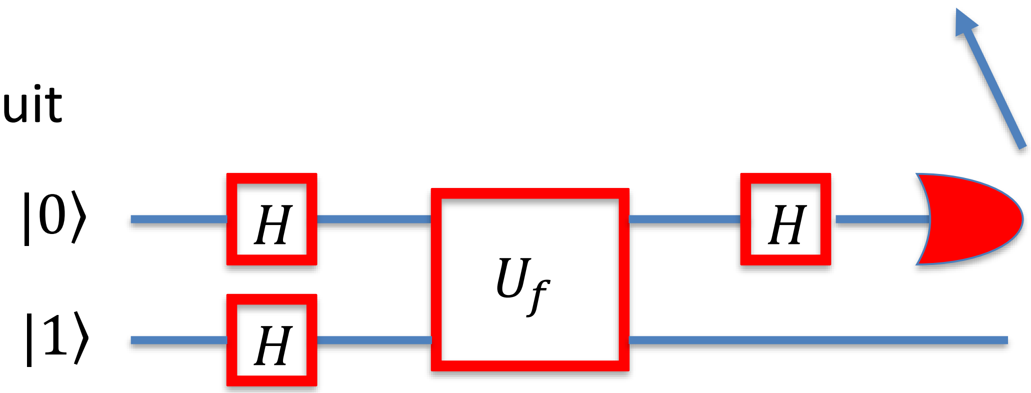
$$((-1)^{f(0)}+(-1)^{f(1)})|0\rangle$$
$$+$$
$$((-1)^{f(0)}-(-1)^{f(1)})|1\rangle$$

Step 4: getting the answer

If $f(0) = f(1)$ → $|0\rangle$

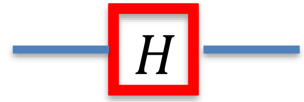
If $f(0) \neq f(1)$ → $|1\rangle$

Deustch circuit



Step 3: quantum data mining

$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$



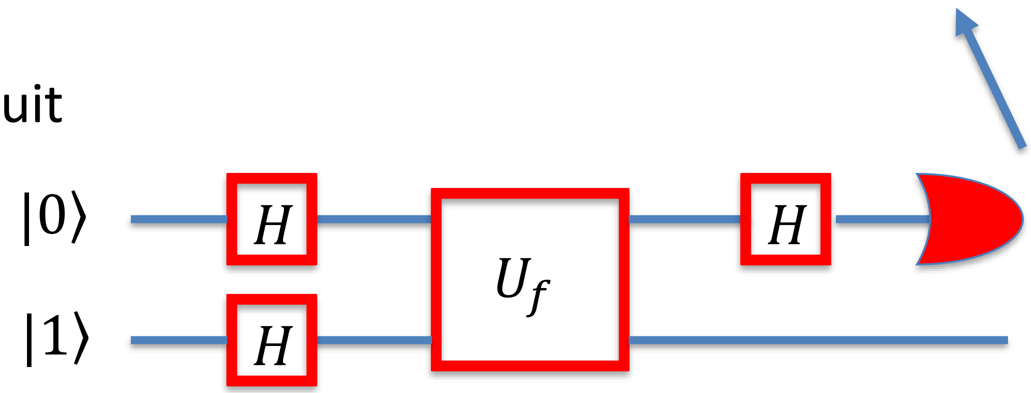
$$((-1)^{f(0)}+(-1)^{f(1)})|0\rangle$$
$$+$$
$$((-1)^{f(0)}-(-1)^{f(1)})|1\rangle$$

Step 4: getting the answer

If $f(0) = f(1)$ → $|0\rangle$

If $f(0) \neq f(1)$ → $|1\rangle$

Deustch circuit



One does not know which constant or balanced is

Step 3: quantum data mining

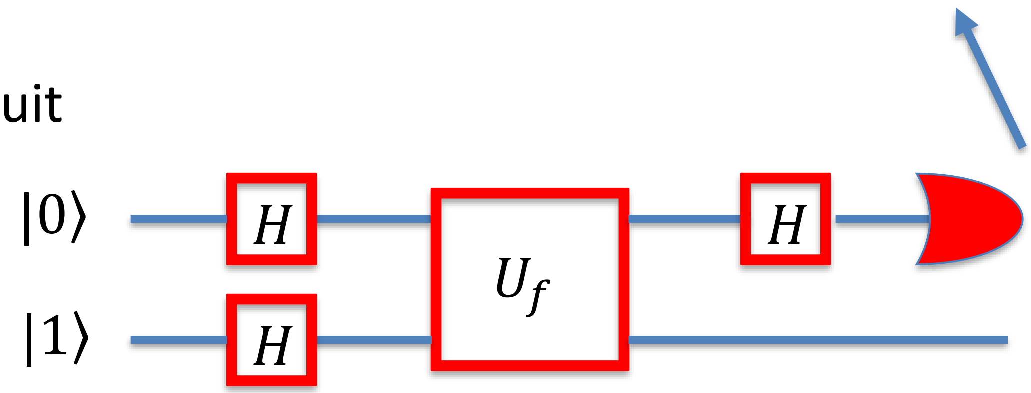
$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \;—\; \boxed{H} \;—\; \begin{matrix} ((-1)^{f(0)}+(-1)^{f(1)})|0\rangle \\ + \\ ((-1)^{f(0)}-(-1)^{f(1)})|1\rangle \end{matrix}$$

Step 4: getting the answer

If $f(0) = f(1)$ → $|0\rangle$

If $f(0) \neq f(1)$ → $|1\rangle$

Deustch circuit

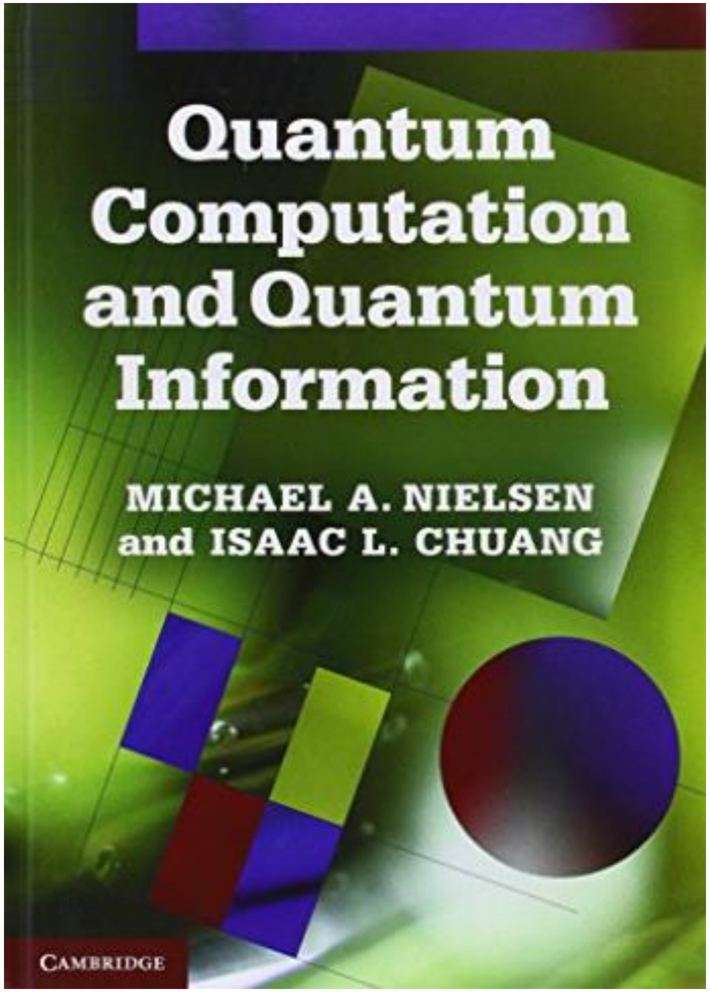


One does not know which constant or balanced is

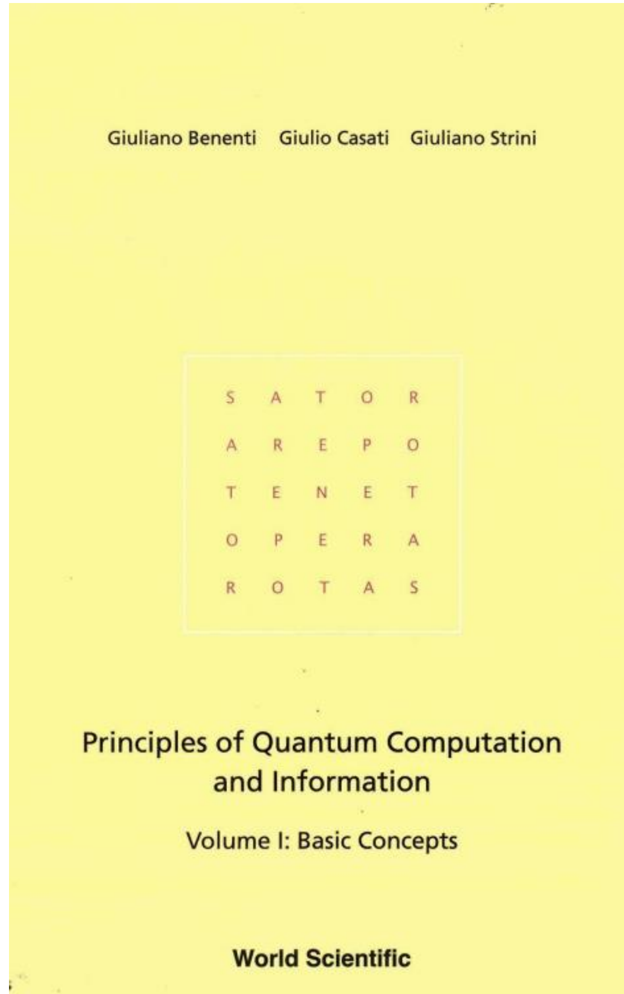
You can't always get what you want
But if you try sometime you find
You get what you need

Rolling Stones

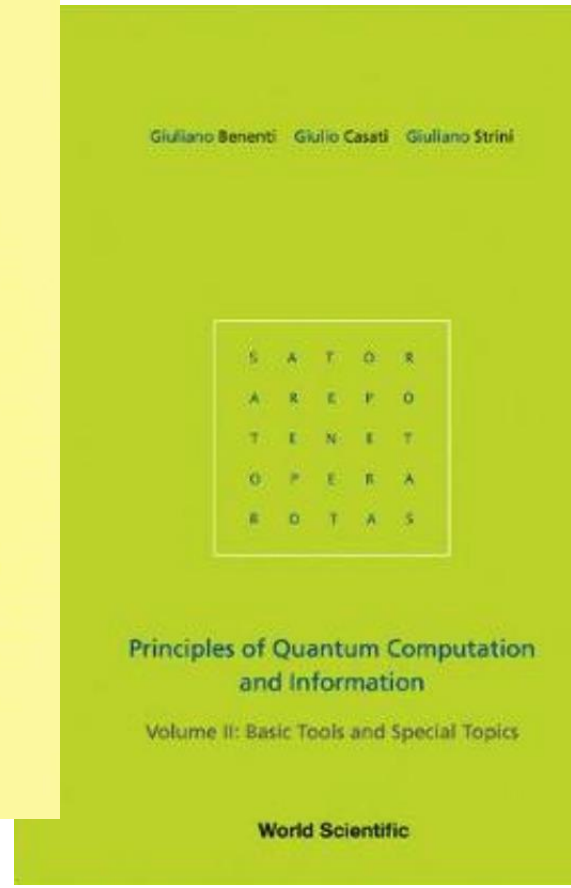
References



Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG
CAMBRIDGE



Giuliano Benenti Giulio Casati Giuliano Strini
S A T O R
A R E P O
T E N E T
O P E R A
R O T A S
Principles of Quantum Computation and Information
Volume I: Basic Concepts
World Scientific



Giuliano Benenti Giulio Casati Giuliano Strini
Principles of Quantum Computation and Information
Volume II: Basic Tools and Special Topics
World Scientific

Thanks so much for your attention

Muchas gracias por su atención