Introduction to Quantum Computing I

Germán Sierra (Instituto de Física Teórica UAM-CSIC)

Universidad Internacional Menéndez Pelayo,
1st September 2020

Plan of the lecture

- **Historial background**
- **Basic concepts: the qubit, quantum gates**
- **Basic quantum circuits**

Quantum Mechanics

Computer Sciences

Quantum Computation and Quantum Information

Information Theory

Cryptography

Quantum Mechanics

Quantum Mechanics

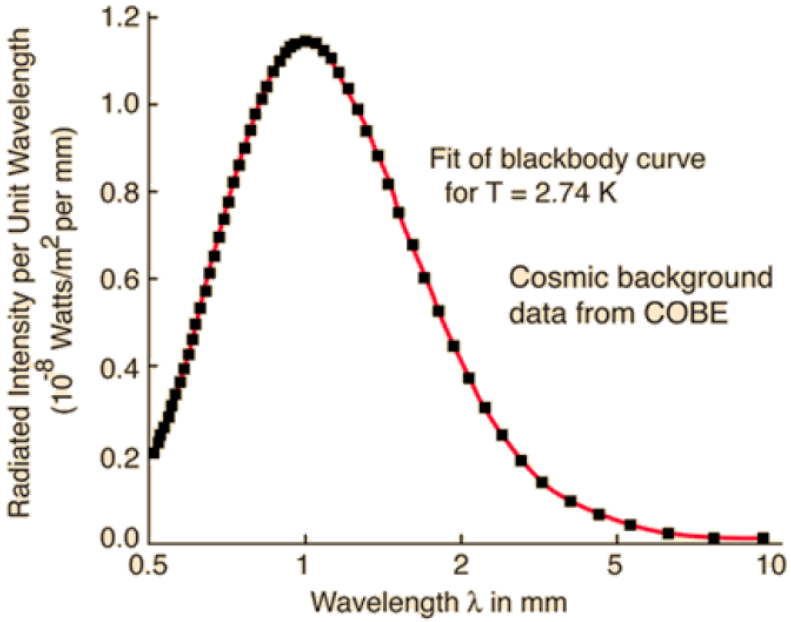
First Quantum Revolution

Max Planck
1858 - 1947

Spectrum of the black body radiation

1900

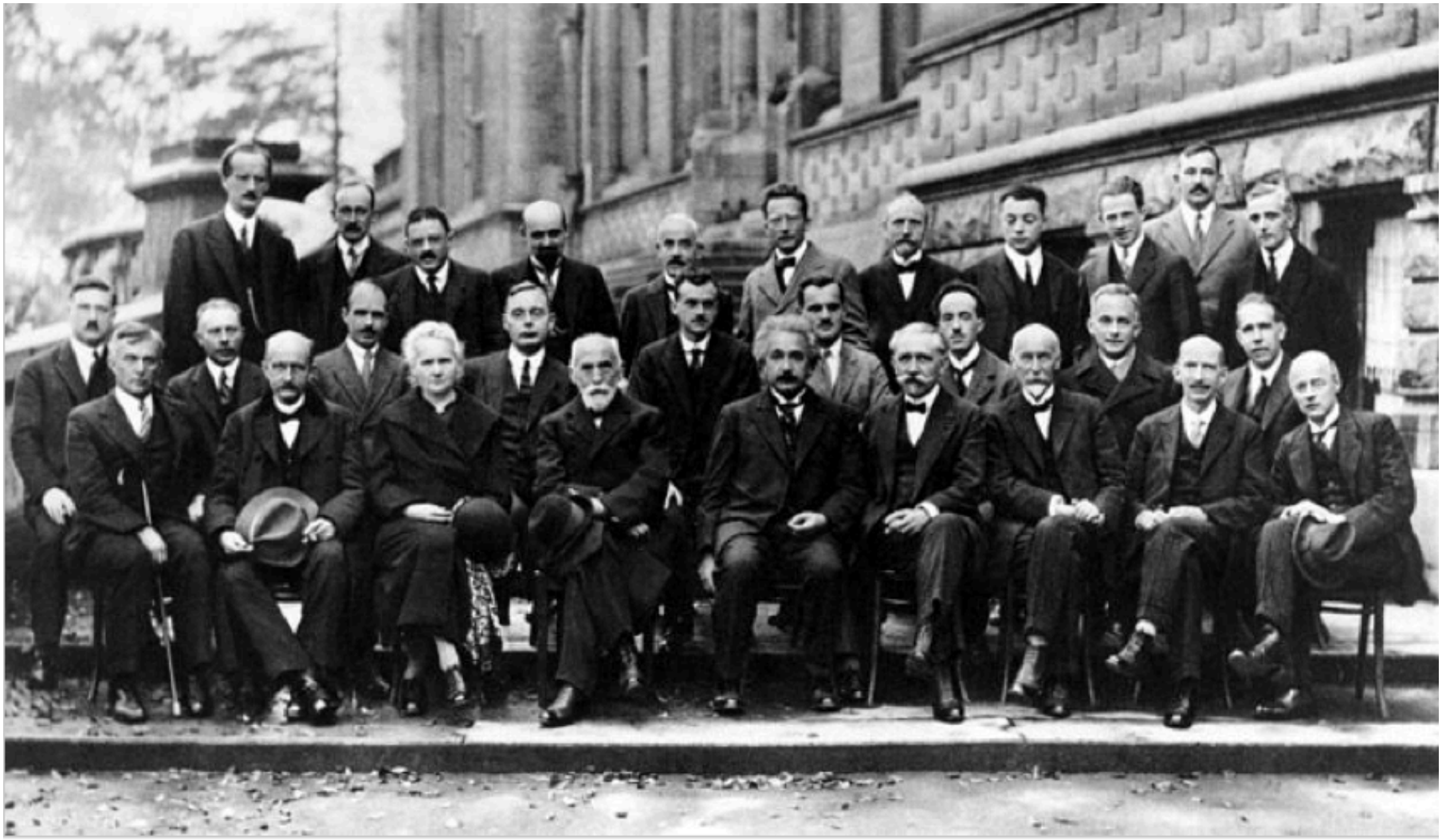
$$u_\nu \, d\nu = \frac{8\pi h \nu^3}{c^3} \cdot \frac{d\nu}{e^{\frac{h\nu}{k\vartheta}} - 1}$$



Quantum of energy

$$E = h\,\nu$$

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

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

Annalen der Physik, 1905

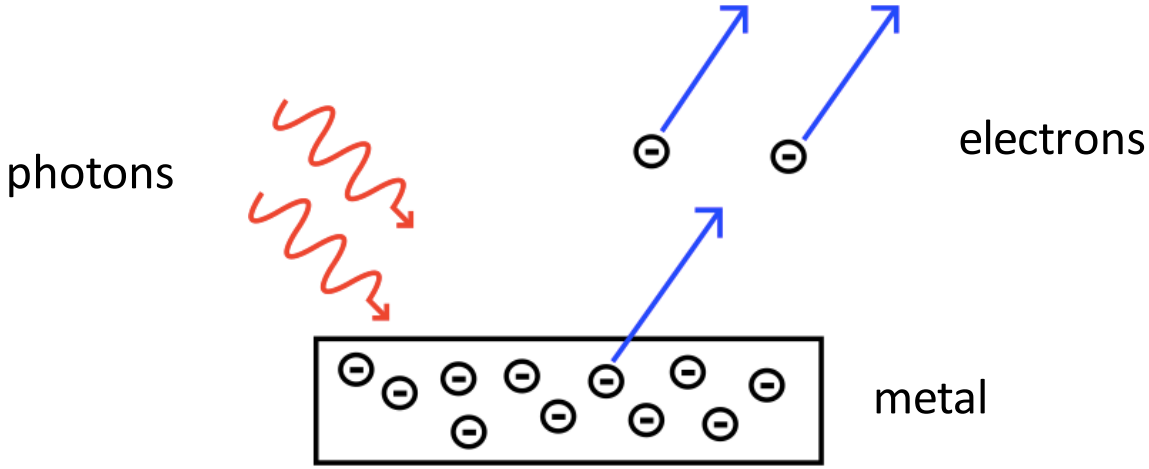
6. *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt;*
von A. Einstein.

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.

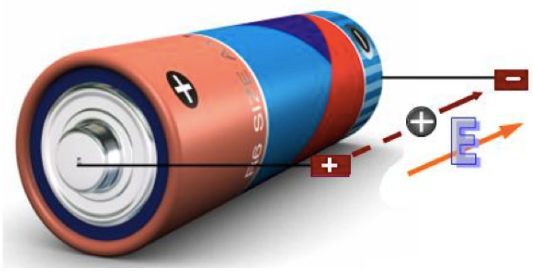
Quantum of light = photon

Photoelectric effect



$$E = h\,f \qquad \text{(Planck 1900)}$$

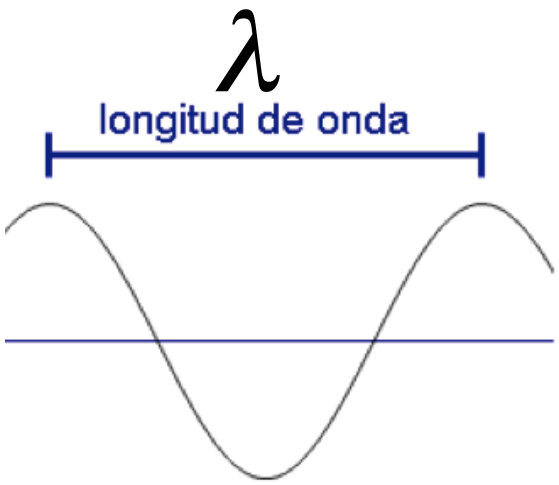
Energy of a yellow photon $E \approx 2$ electrón-voltios



Louis de Broglie
1892-1987

Werner Heisenberg
1901- 1976

Particles are also waves



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

Matrix Mechanics / uncertainty principle

$$[x, p] = i\,\hbar$$

$$\Delta x \, \Delta p \geq \frac{\hbar}{2}$$

Erwin Schrödinger
1887 - 1961

Max Born
1882 - 1970

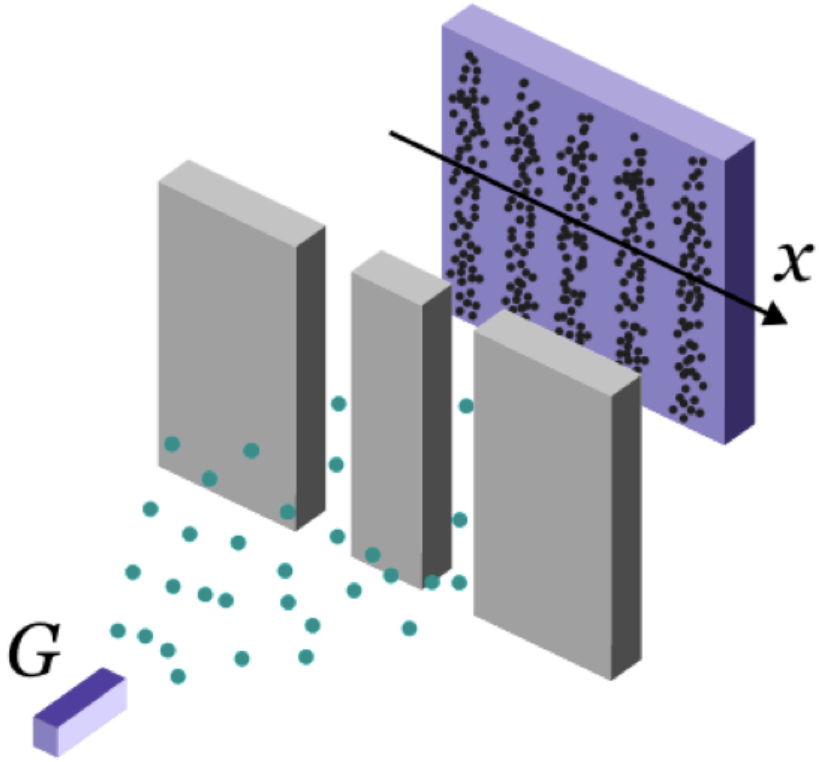
Wave function / Time evolution

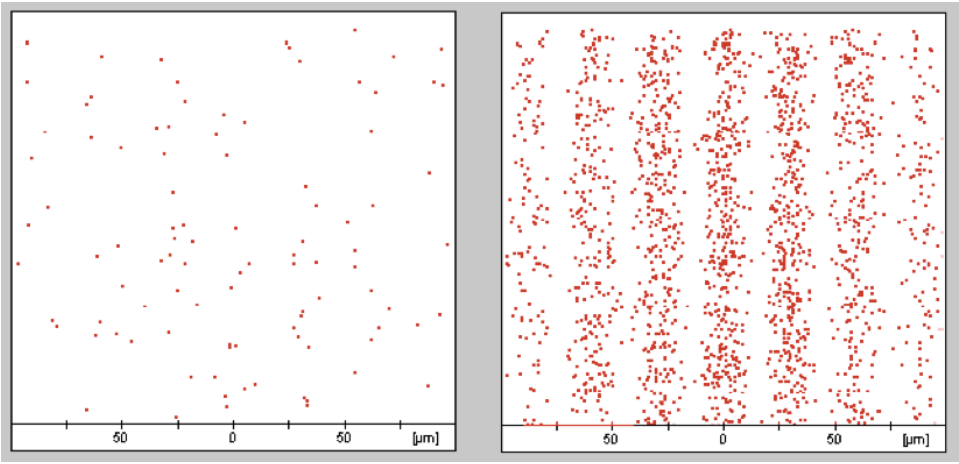
$$i\,\frac{\partial\psi}{\partial t} = \left(-\frac{\hbar^2\nabla^2}{2m} + V(\vec{x})\right)\psi$$

Probabilistic interpretation

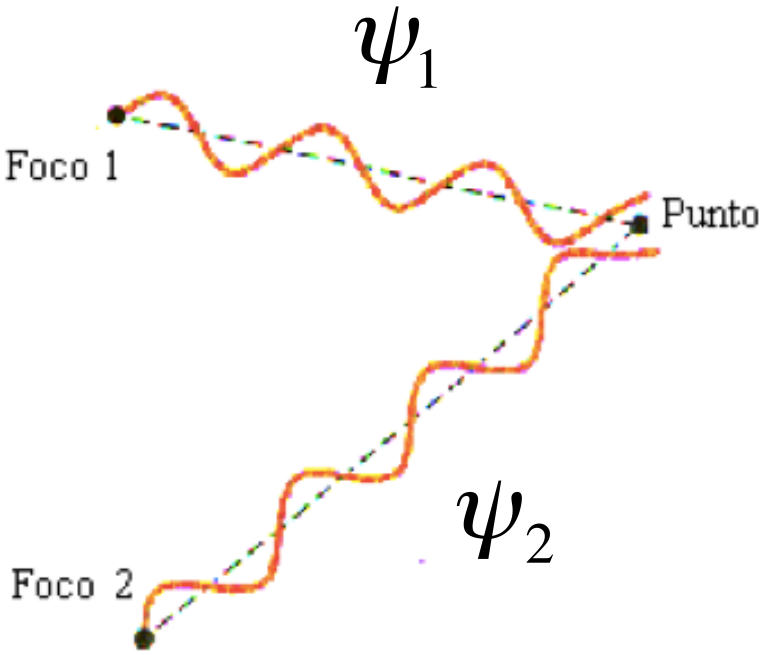
$$\frac{dP}{dV} = |\psi(\vec{x})|^2$$

Particle-wave duality: Double slit experiment with electrons

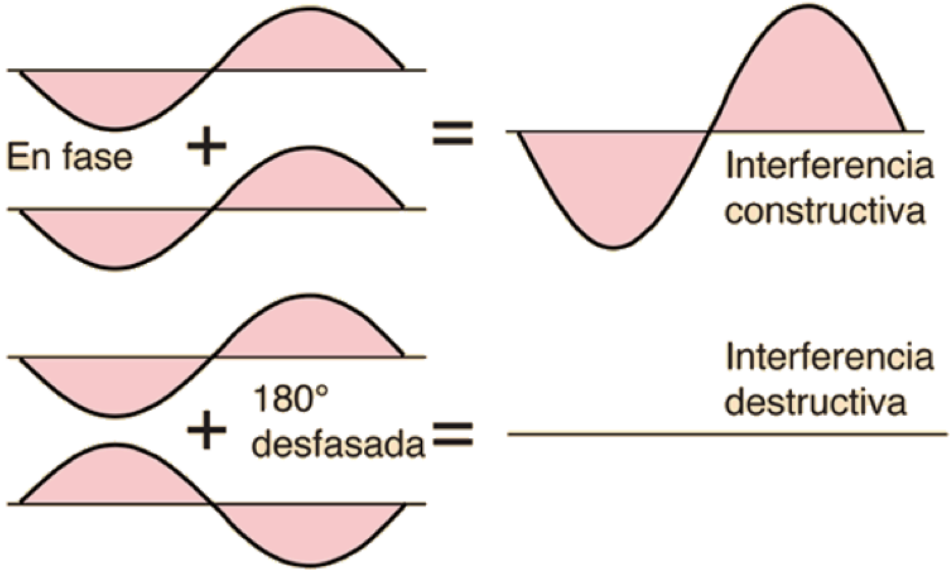




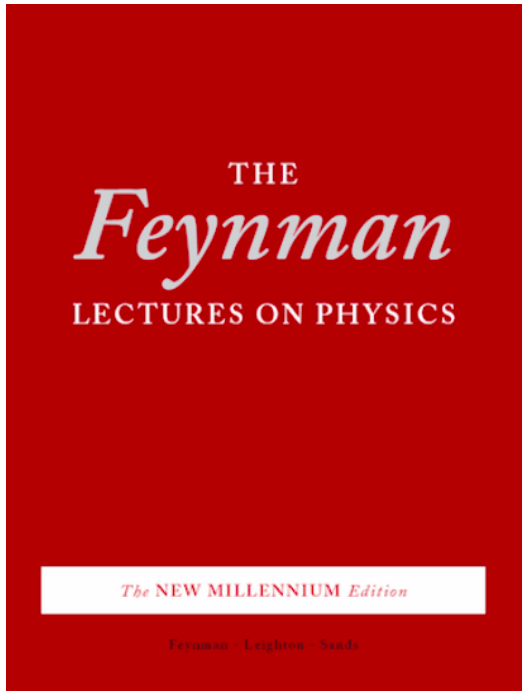
Superposition principle: Interference



$$\psi_1 + \psi_2$$



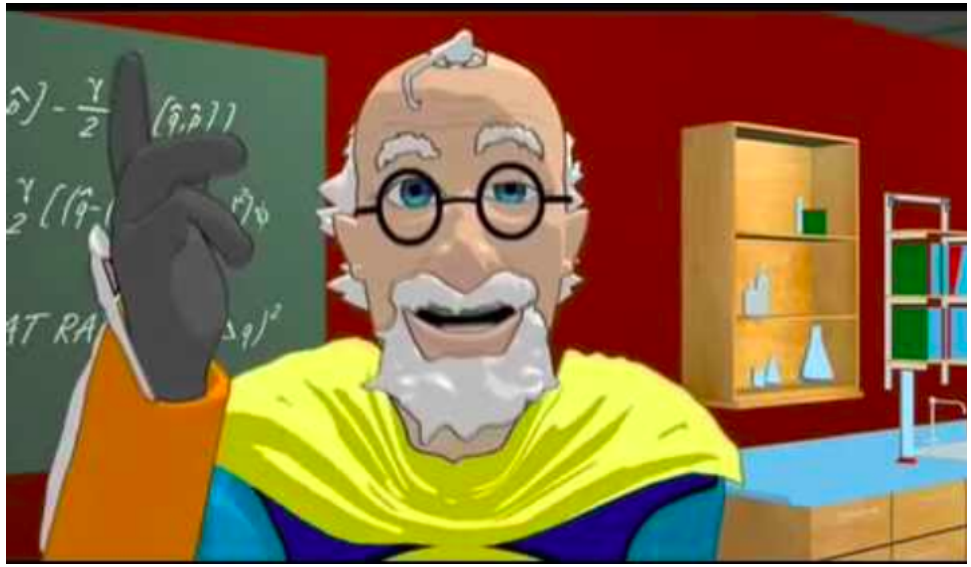
Richard Feymann : Quantum Mechanics can be understood by giving it a lot of thought
1918 - 1988 to the double slit experiment



See in YouTube

Dr. Quantum – Double Slit experiment

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

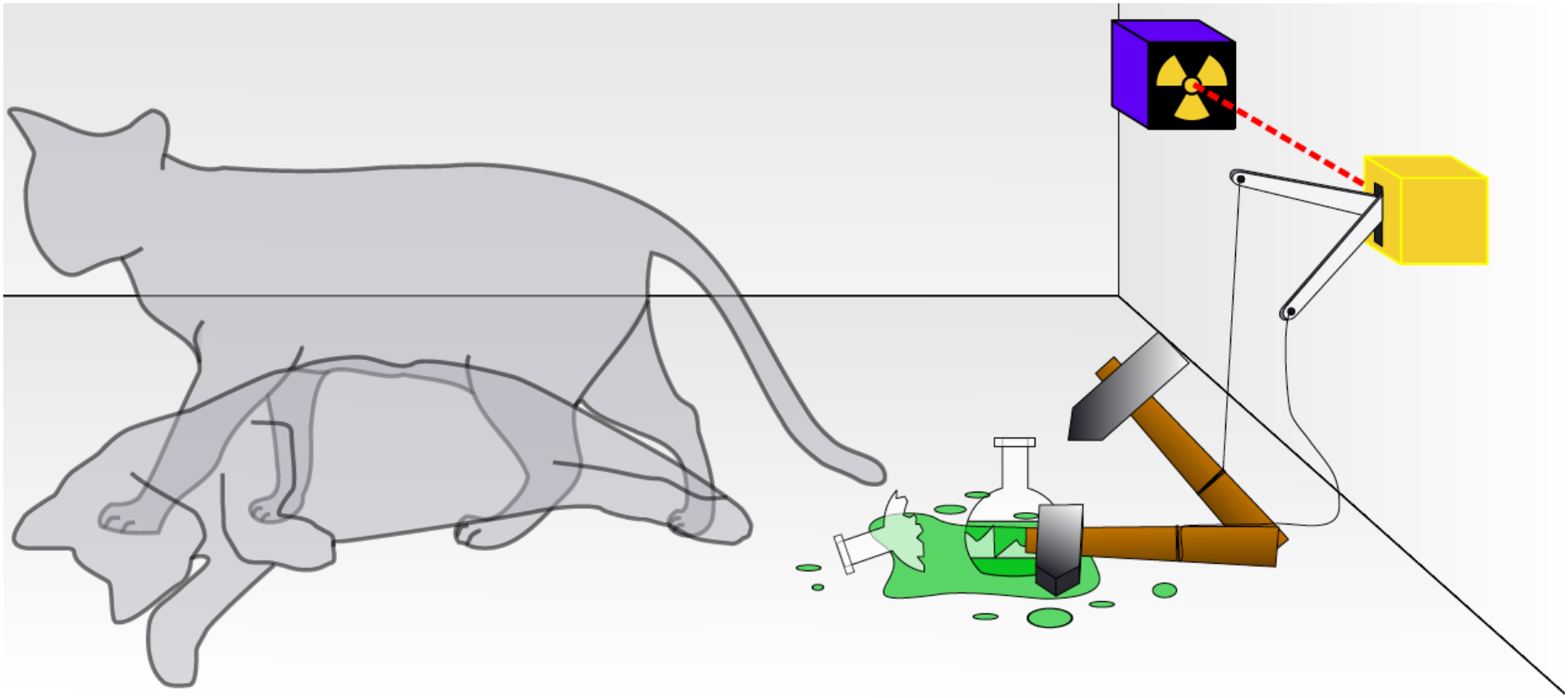


Cartoon picture of the double slit experiment

“Quantum” Skier

Classical Observer

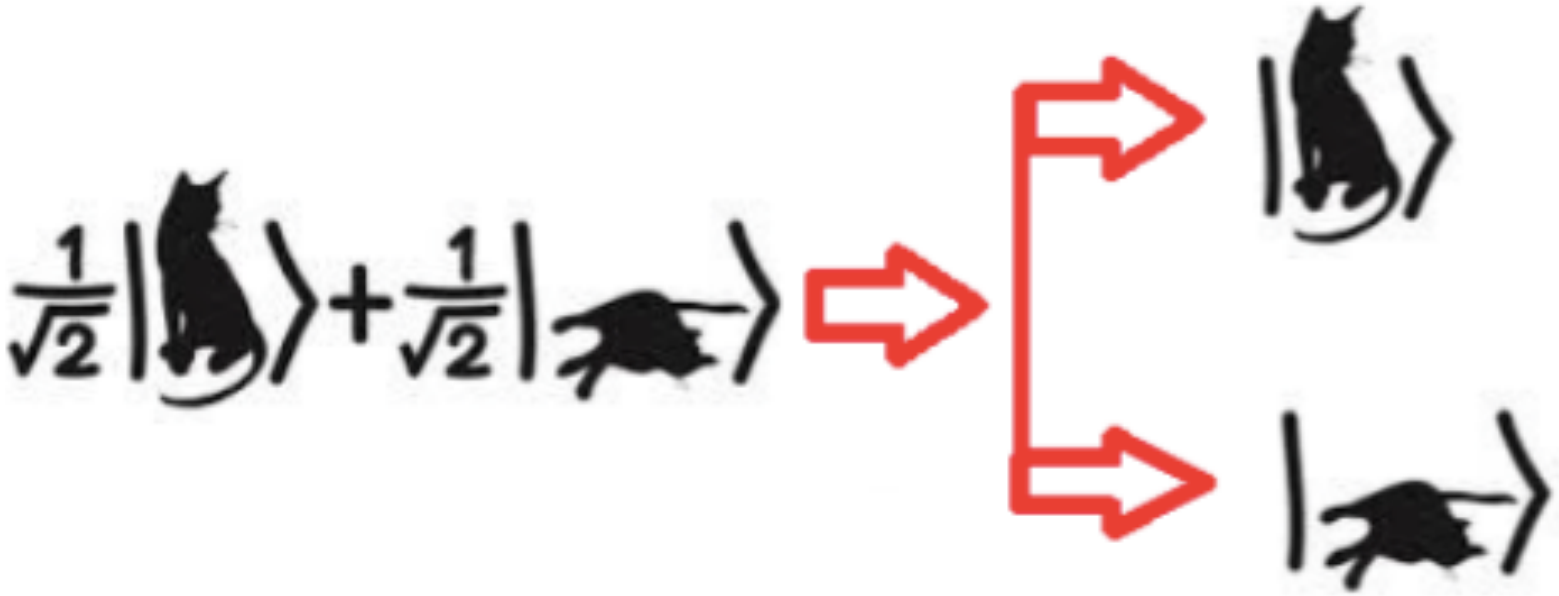
Paradox: Schrödinger cat (1935)



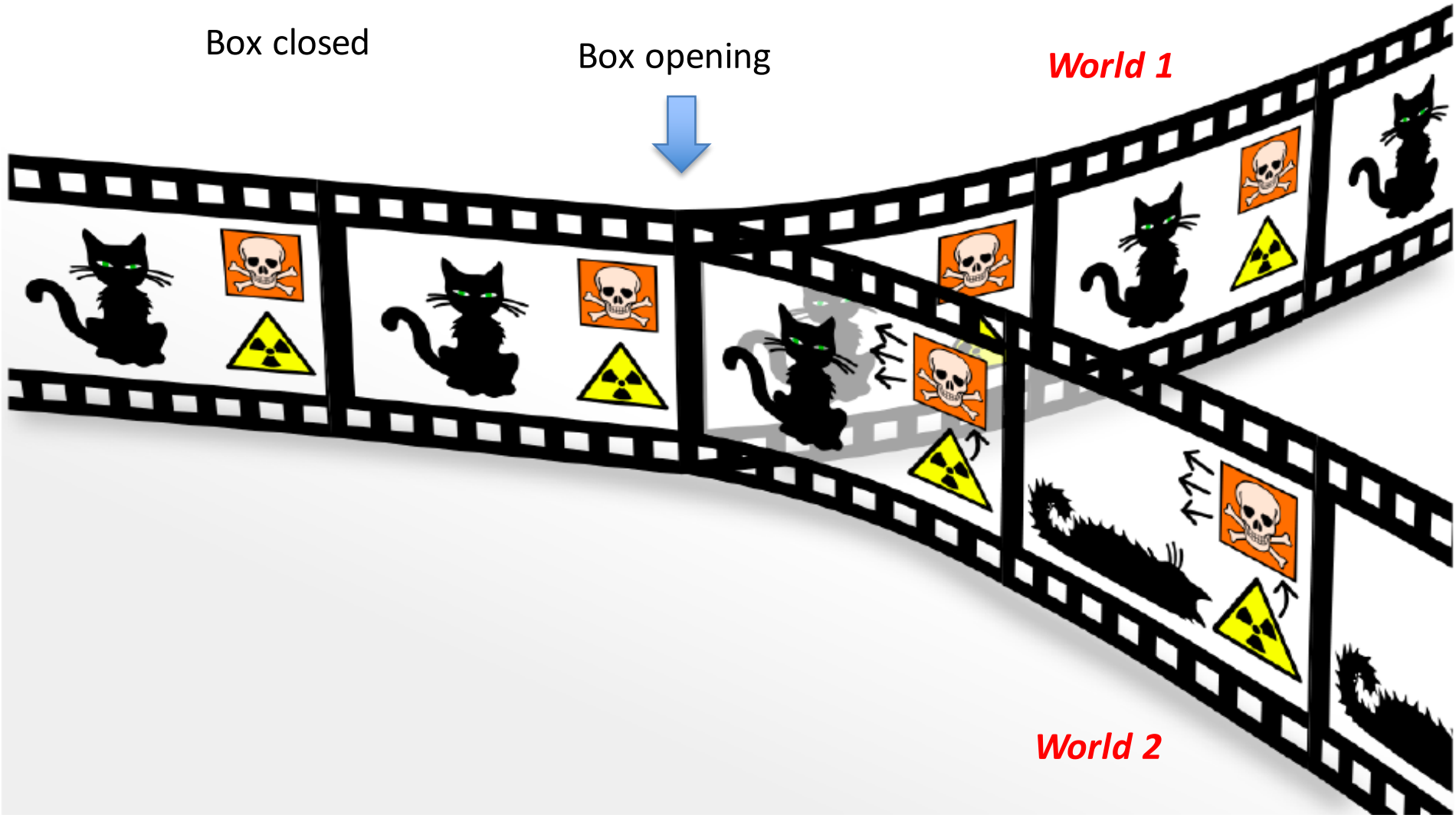
$$\psi = \textit{Dead} + \textit{Alive}$$

Copenhagen interpretation

Opening the box produces the COLLAPSE of the wave function

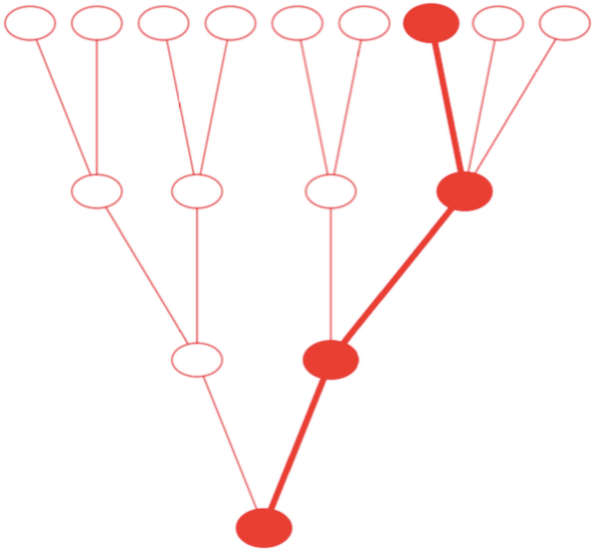


Many world interpretation



Many world interpretation: Hugh Everett (1957)

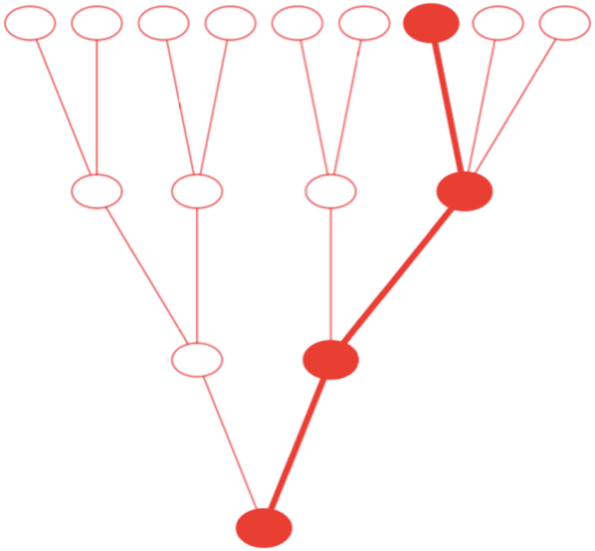
time



Hugh Everett
1930 - 1982

Many world interpretation: Hugh Everett (1957)

time



Hugh Everett
1930 - 1982

Anticipated in literature by Borges

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

Cuento ***"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, 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)

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)

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

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)

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

Hidden variable theories

Two interpretation of the physical reality

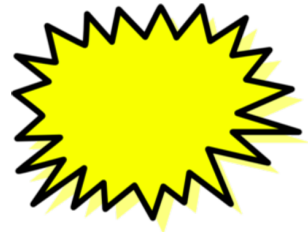
Local Realism

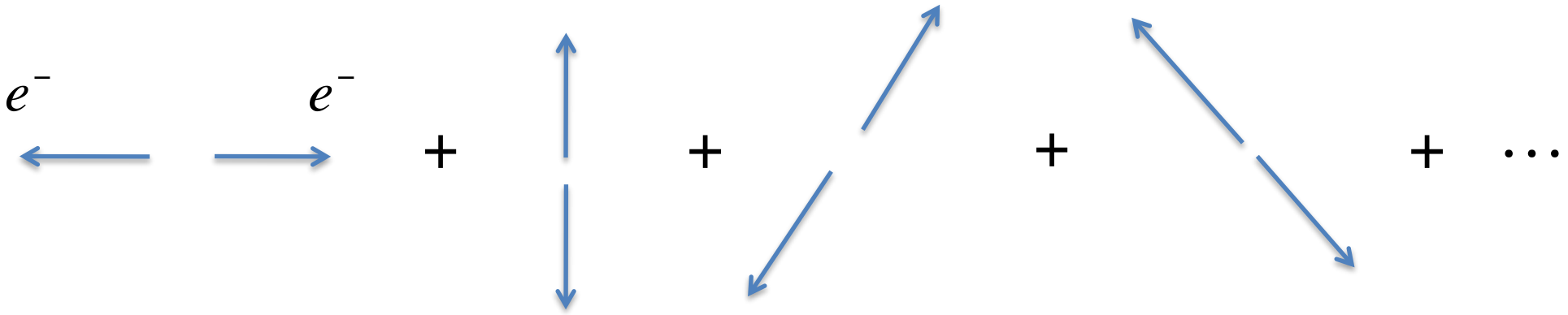
The observable quantities have a value prior to their measurement

Quantum Mechanics

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

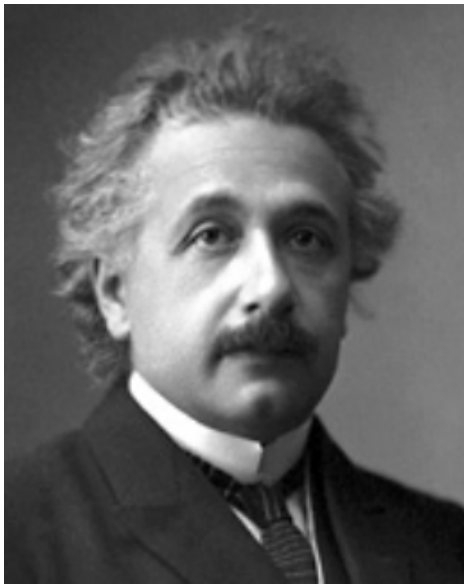
EPR : Gedanken experiment

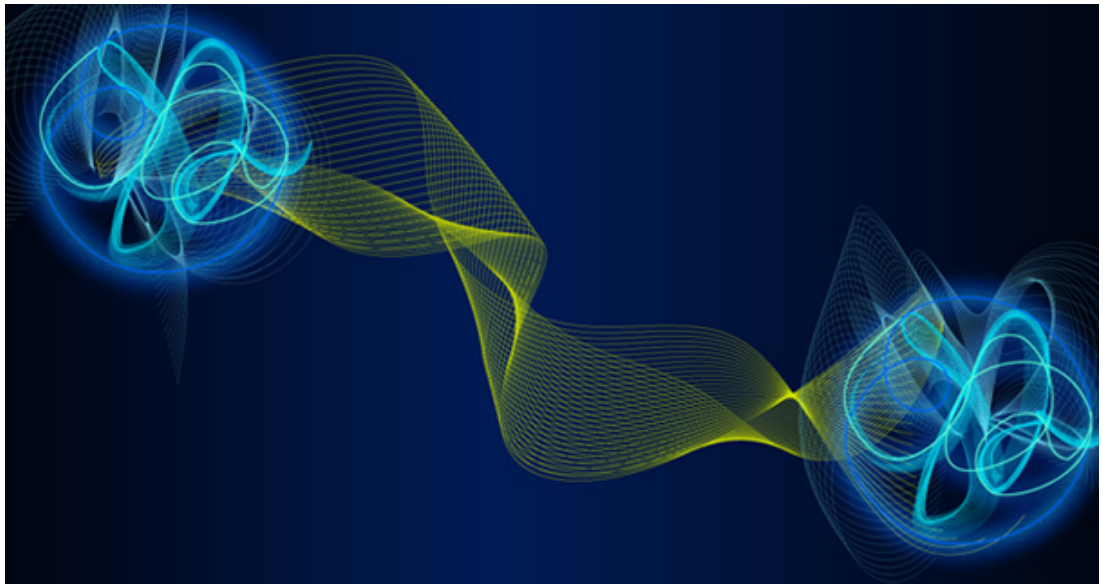




Superposition of two electron with opposite momentum

Spooky action at a distance





Schrödinger called it ENTANGLEMENT (1935)

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 construction of hidden variable theories

Theory of “pilot waves” of de Broglie and Bohm

John von Neumann
1903-1957

von Neumann theorem:

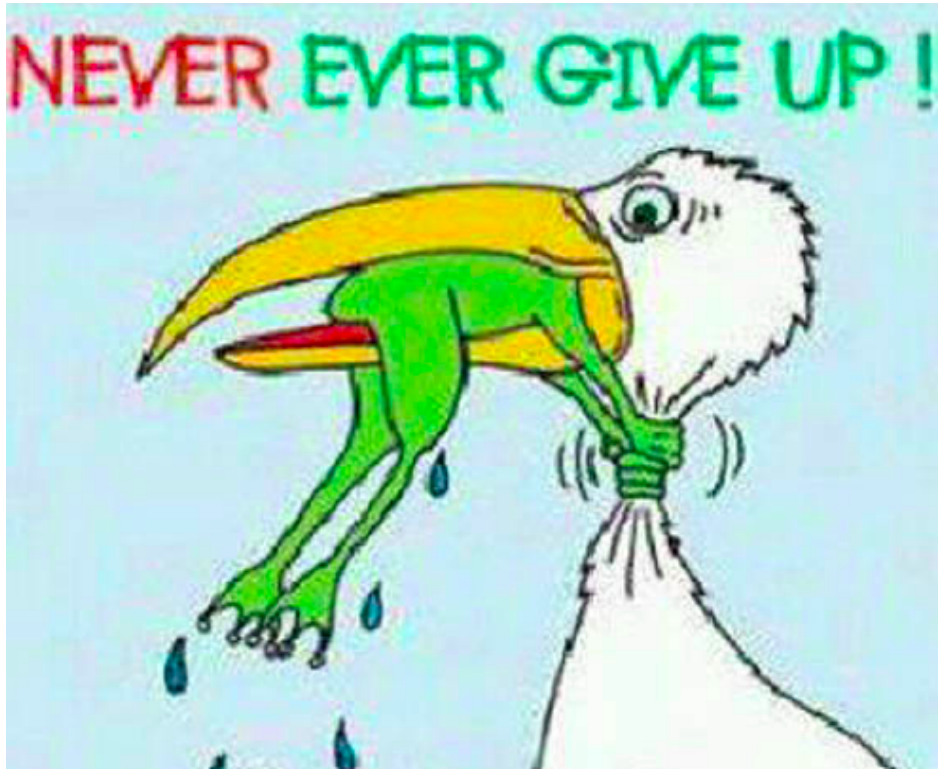
Hidden variable theories are incompatible with Quantum Mechanics

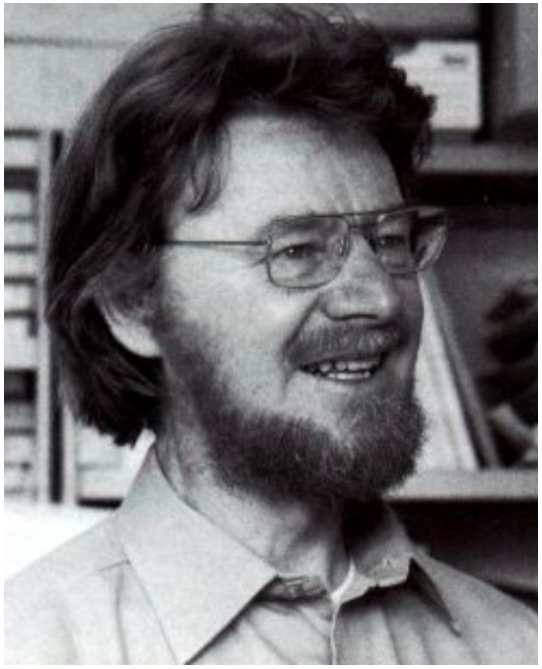
After this discussion a DICTUM was imposed

"Shut up and calculate"

After this discussion a DICTUM was imposed

"Shut up and calculate"





John Bell
1928-1990

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

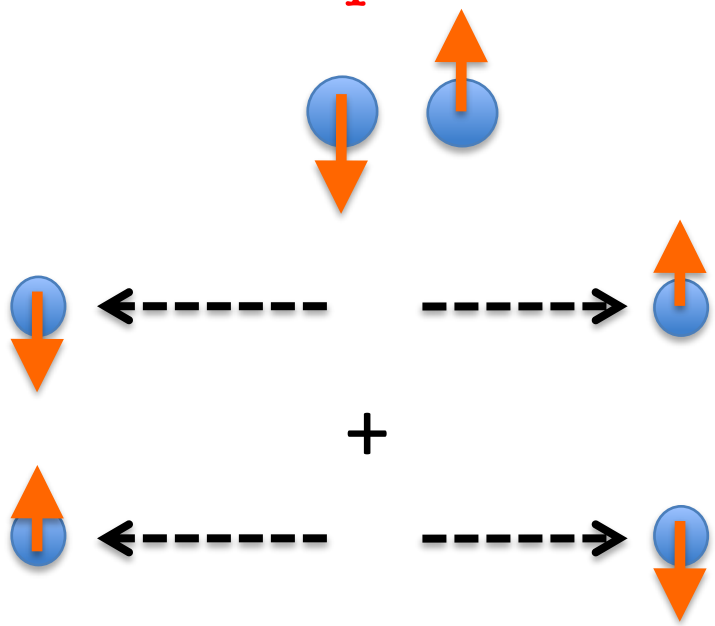
EPR ideas were not a mere philosopical speculation
about the interpretation of Quantum Mechanics

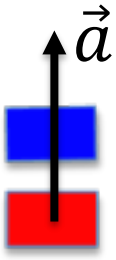
It would be possible to falsify "local realism" with an experiment

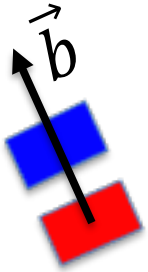
Bell inequalities (1964)

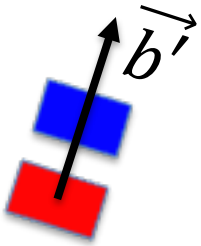
Bell experiment

EPR pair of spins









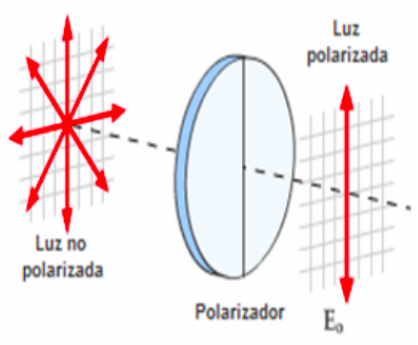
Local realism ⟹ $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{b}')| \leq 1 + P(b,\vec{b}')$

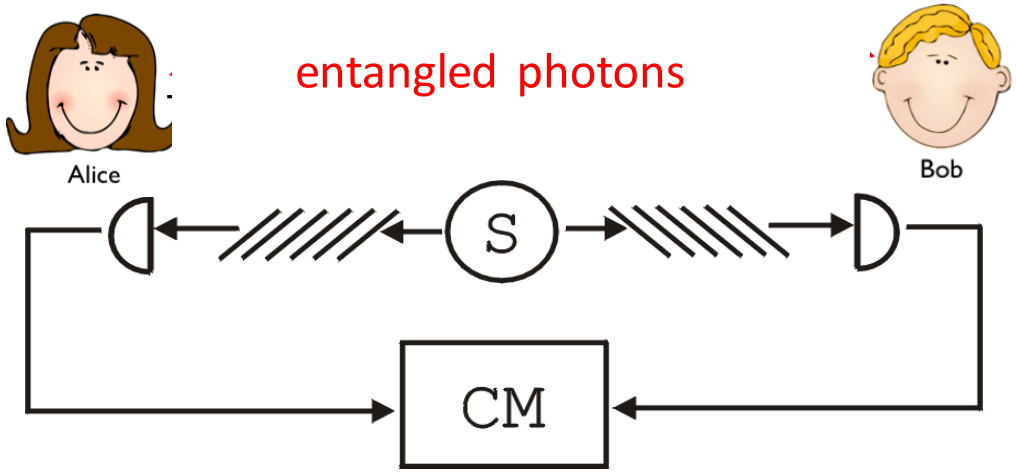
Quantum Mechanics $P(\vec{a},\vec{b}) = -\vec{a} \cdot \vec{b}$ can violate this inequality

Experiments to verify Bell's inequality

- electrons -> photons

- spin -> polarization





Coincidence Monitor

Aspect's experiments (1981)

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

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

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

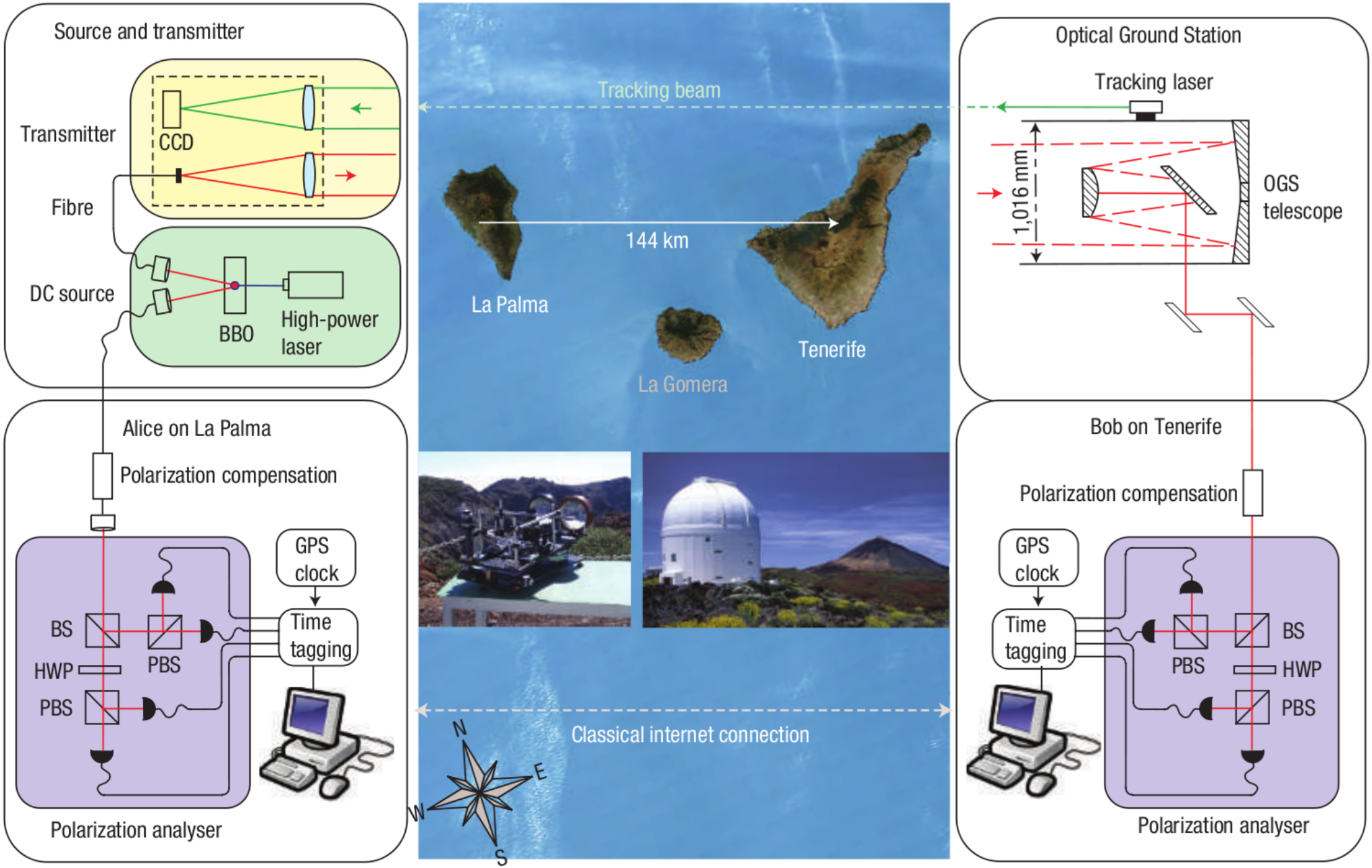
Alan Aspect
1947

~~***LOCAL REALISM***~~

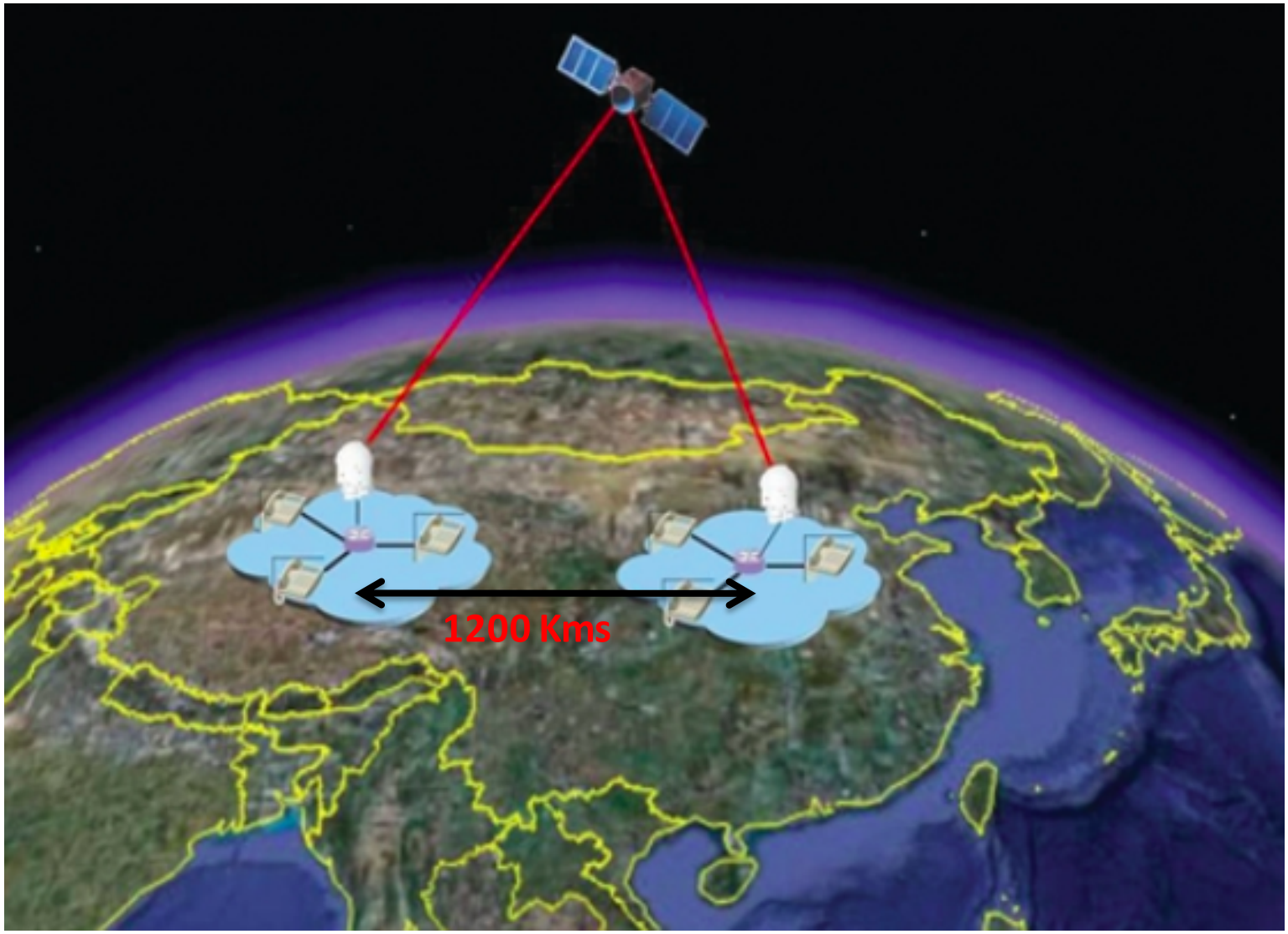
Bell experiment in Austria, Innsbruk (1998)

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

Bell experiment in Canary islands (2007)



QESS (Quantum Entanglement at Space Scale) 2016-2018



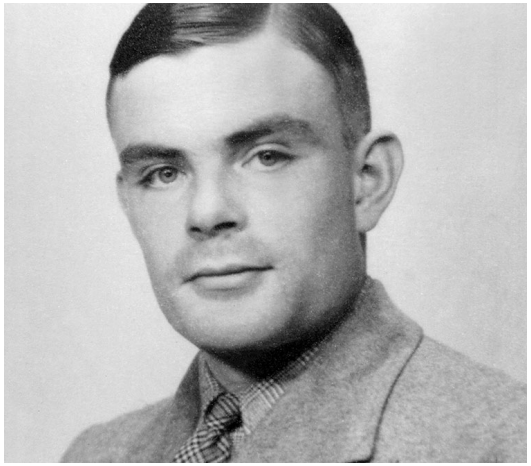
Joint Proyect China and Austria

Quantum Mechanics

Computer Sciences

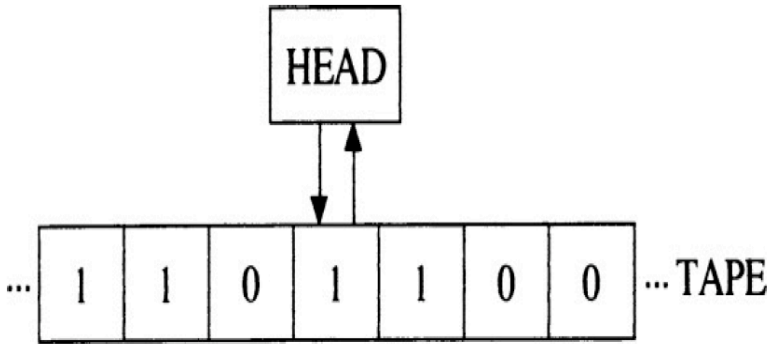
Quantum Computation and Quantum Information

Computer Sciences



Alan Turing (1914-1944)

Turing machine

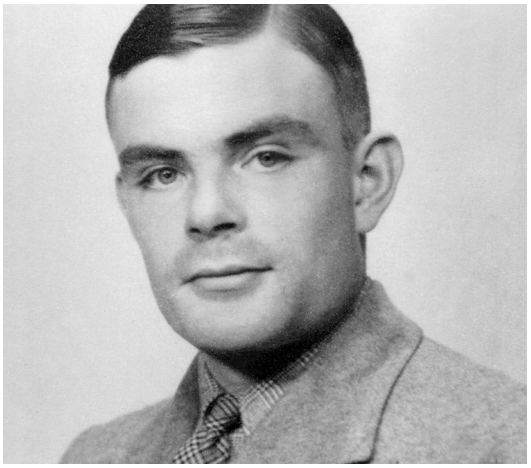


Program :

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

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

Alonzo Church (1903-1995)



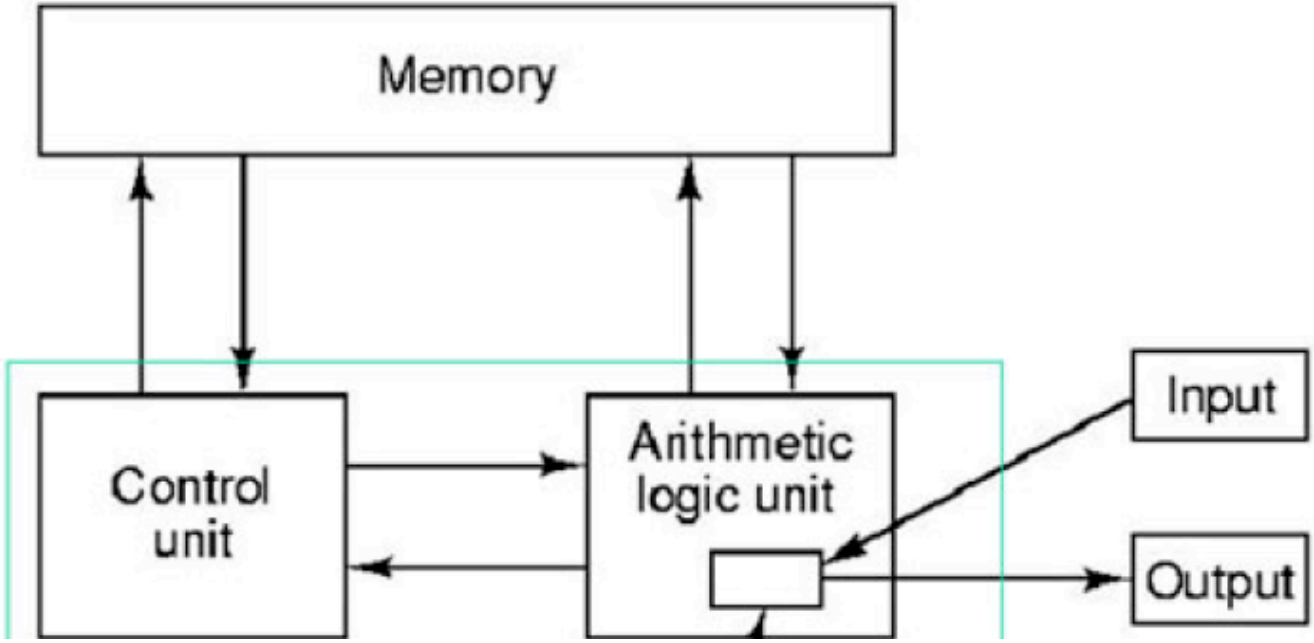
Alan Turing (1914-1944)

The Church-Turing thesis (1936)

Any algorithmic process can be simulated efficiently using a Turing machine

John von Neumann
1903-1957

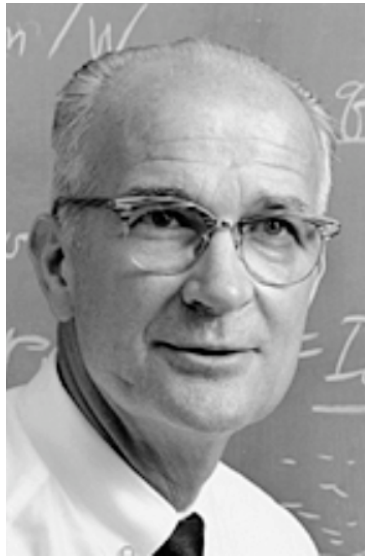
The architect of the computers



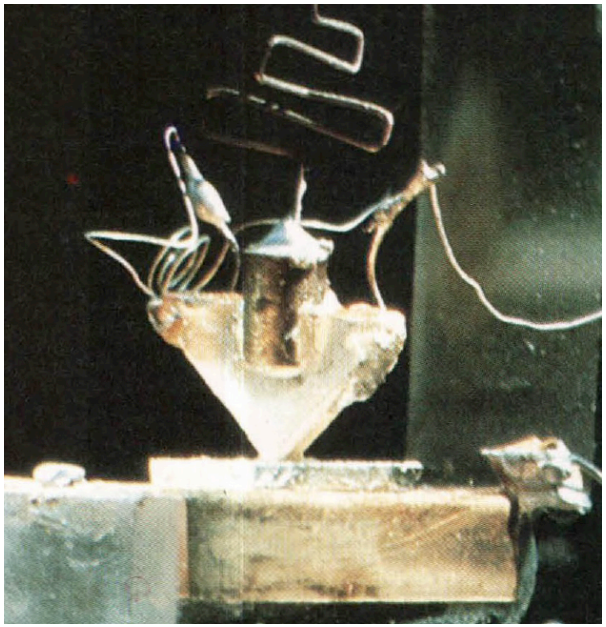
The first transistor (1947)

John Bardeen
1908-1991

Walter Brattain
1902-1987

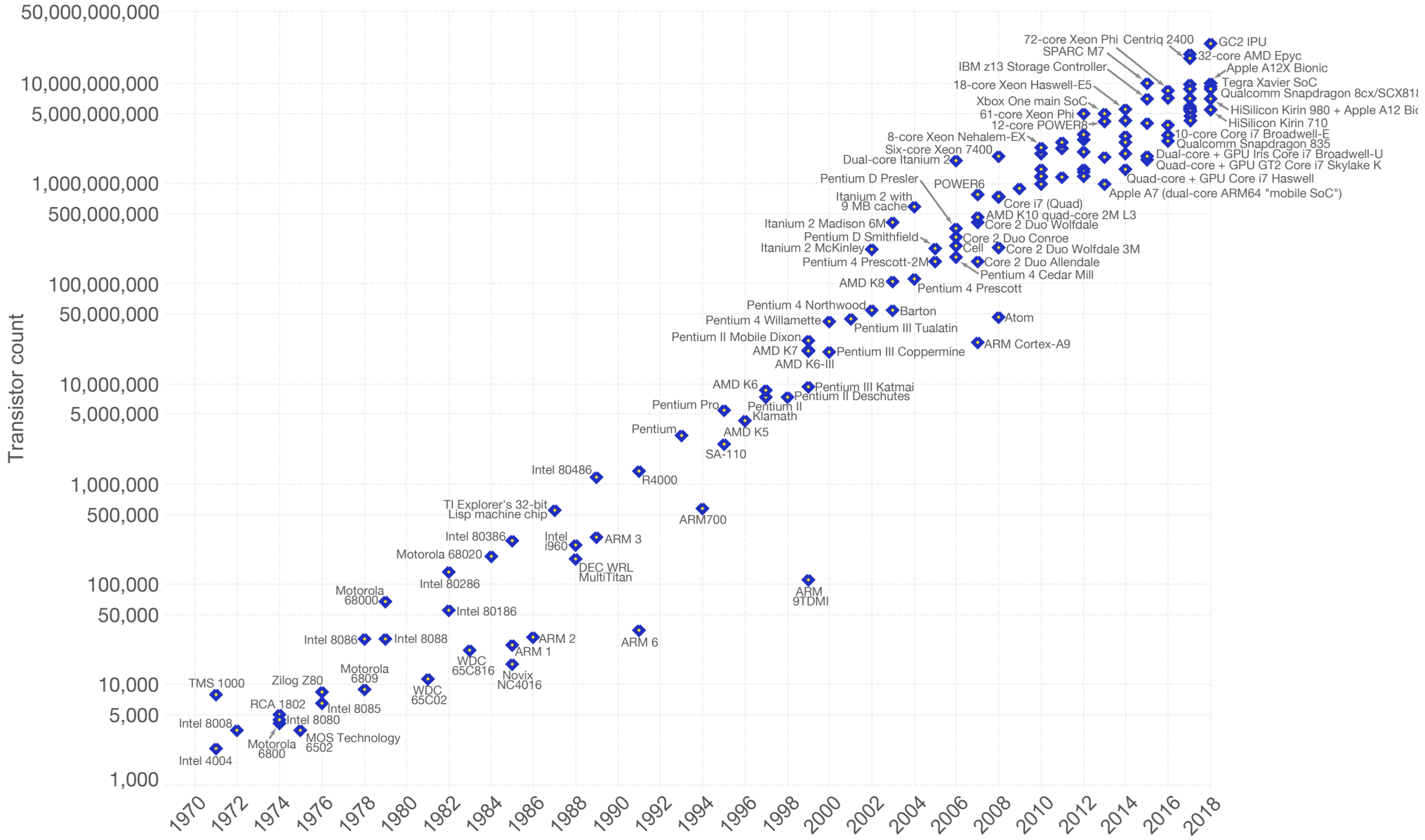


William Schockely
1902-1987



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.



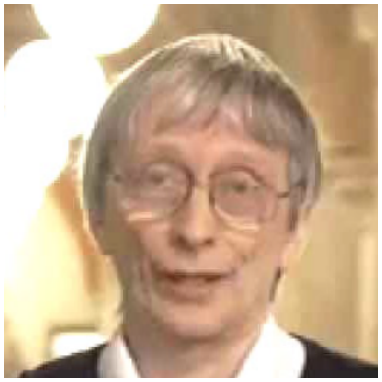
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

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

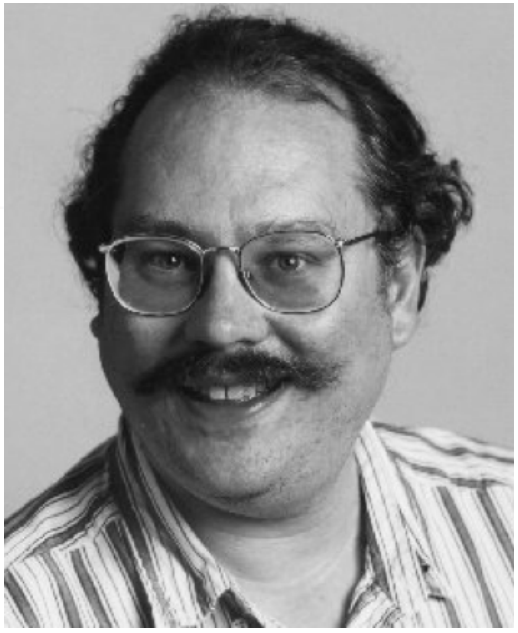
1985

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)

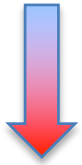


Peter Shor 1959

Prime factorization can be done in polynomial time
In a quantum computer

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

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

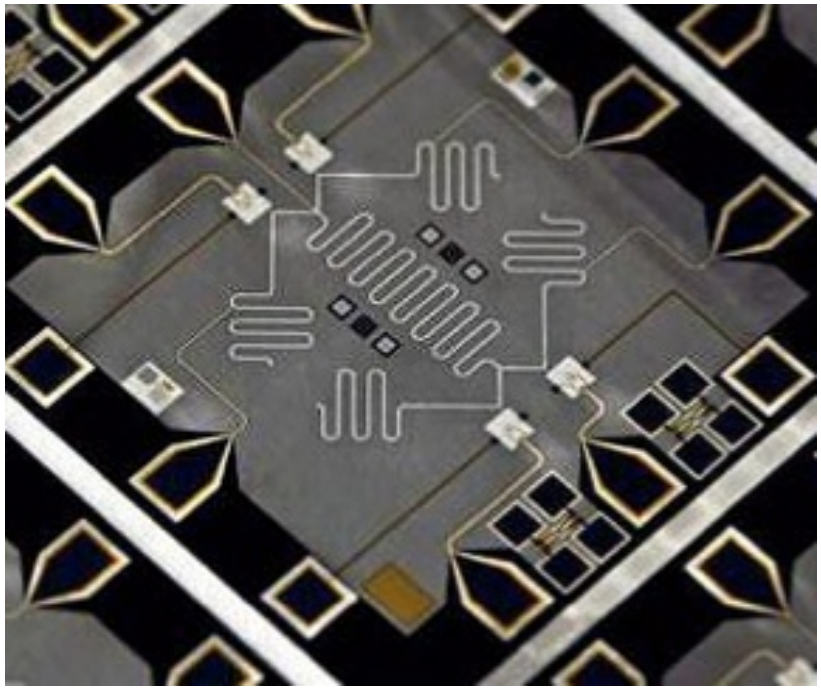


Exponential speedup

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

15 = 3 x 5

Proof of principle



University of California at Santa Barbara 2012

A theoretical estimation (Fowler et al 2012)

n=2000 bits -> 4000 logical qubits -> 2 x 10^8 physical qubits -> 1 day

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

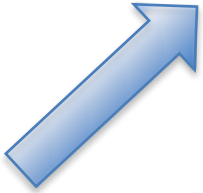
In a quantum computer it takes order $\sqrt{N}$

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

Quantum Mechanics

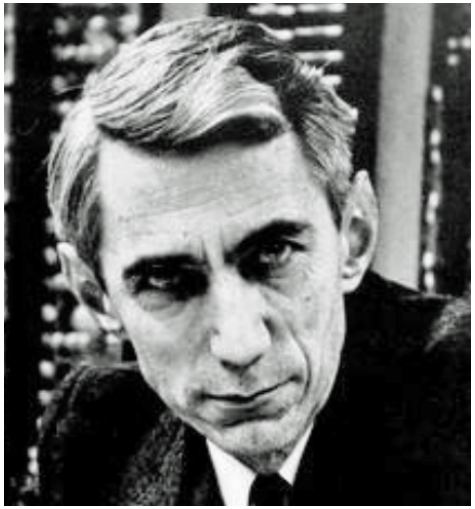
Computer Sciences

Quantum Computation and Quantum Information



Information Theory

Information theory

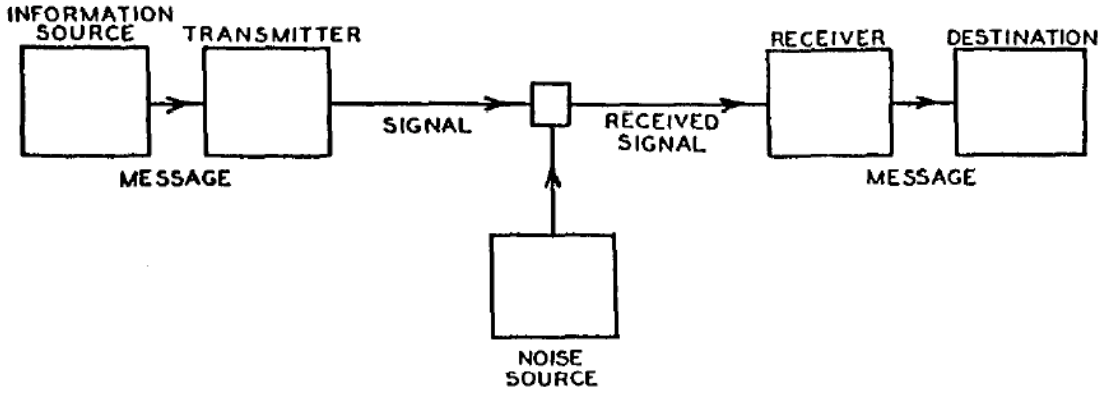


Claude Shannon
1916-2001

A Mathematical Theory of Communication

By C. E. SHANNON

Published in The Bell System Technical Journal 1948



Capacity of a communication channel

$$C = \operatorname{Lim}_{T \to \infty} \frac{\log N(T)}{T}$$

Measure of information: Entropy

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

Noiseless channel coding theorem

Noisy channel coding theorem

Error correcting codes

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”

Quantum error correction

No cloning theorem forbids to use redundancy for QEC: you cannot copy a quantum state

Scheme for reducing decoherence in quantum computer memory

Peter W. Shor*

1995

$$|0\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)$$

Quantum Mechanics

Computer Sciences

Quantum Computation and Quantum Information

Information Theory

Cryptography

Cryptography

Private key cryptography

Kv fvb svcl tl?

Do you love me? E D

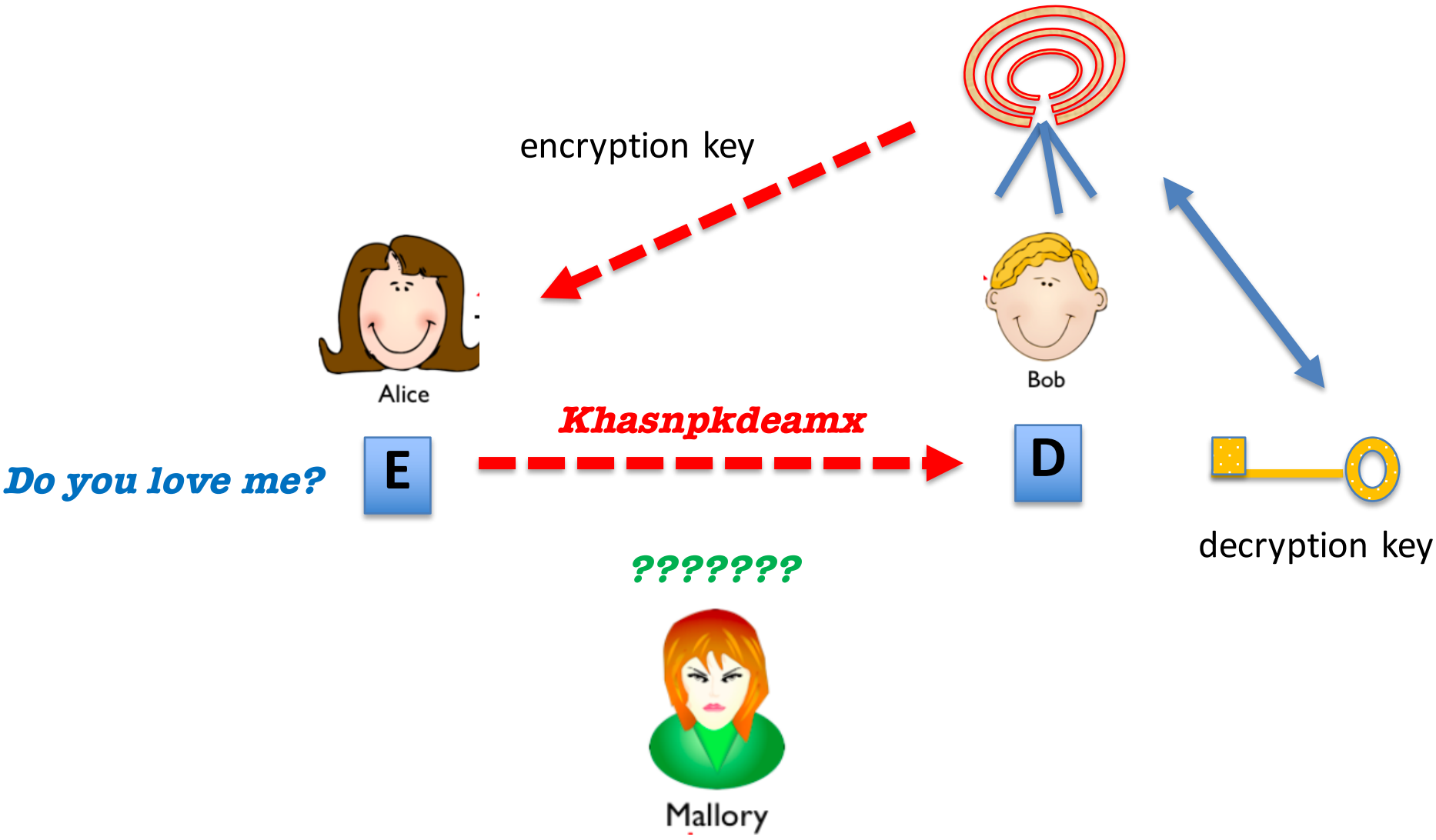
$7: a \rightarrow h$

Vm jvbyzl

P kv uva

Julius Caesar
100-44 BC

Public key cryptography



Public key cryptography 1970's

Whitfield Diffie 1944

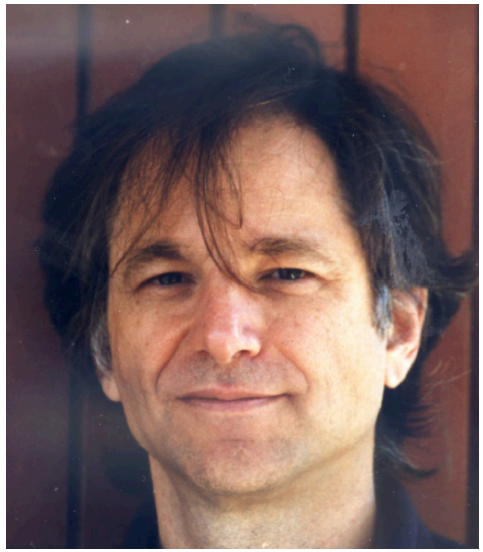
Martin Hellman 1945

Ralph Merkle 1952

RSA protocol 1977

Ronald Rivest 1947

Ad Shamir 1952



Leonard Adleman 1945

Largest RSA number that has been factored :
250 decimal digits (829 bits) by F. Boudot, et al (Feb 2020)

RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937

RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
023862359875266834770873766192558569463979885336 7 ×
333720275949781565562260106053551142279407603447675546667845209870238417292100370802574486732968818775657189862580369320627 11

RSA-260 has not been factored so far.

RSA-260 = 2211282552952966643528108525502623092761208950247001539441374831912882294140
200198651272972656974659908590033003140005117074220456085927635795375718595429888389587092292384910067030341246205457845664136645406842143612930176940208463910658759147942514351444581 99

Largest RSA number that has been factored :
250 decimal digits (829 bits) by F. Boudot, et al (Feb 2020)

RSA-250 = 21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979 37

RSA-250 = 64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367 × 33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

RSA-260 has not been factored so far.

RSA-260 = 22112825529529666435281085255026230927612089502470015394413748319128822941402001986512729726569746599085900330031400051170742204560859276357953757185954298838958709229238491006703034124620545784566413664540684214361293017694020846391065875914794251435144458199

Shor's algorithm wiould be able to factorize these numbers quickly
But you will need a large quantum computer

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

First ideas on quantum cryptography

Preprint in late 60's and rejected for publication. It was published in 1983

Charles Bennet 1943

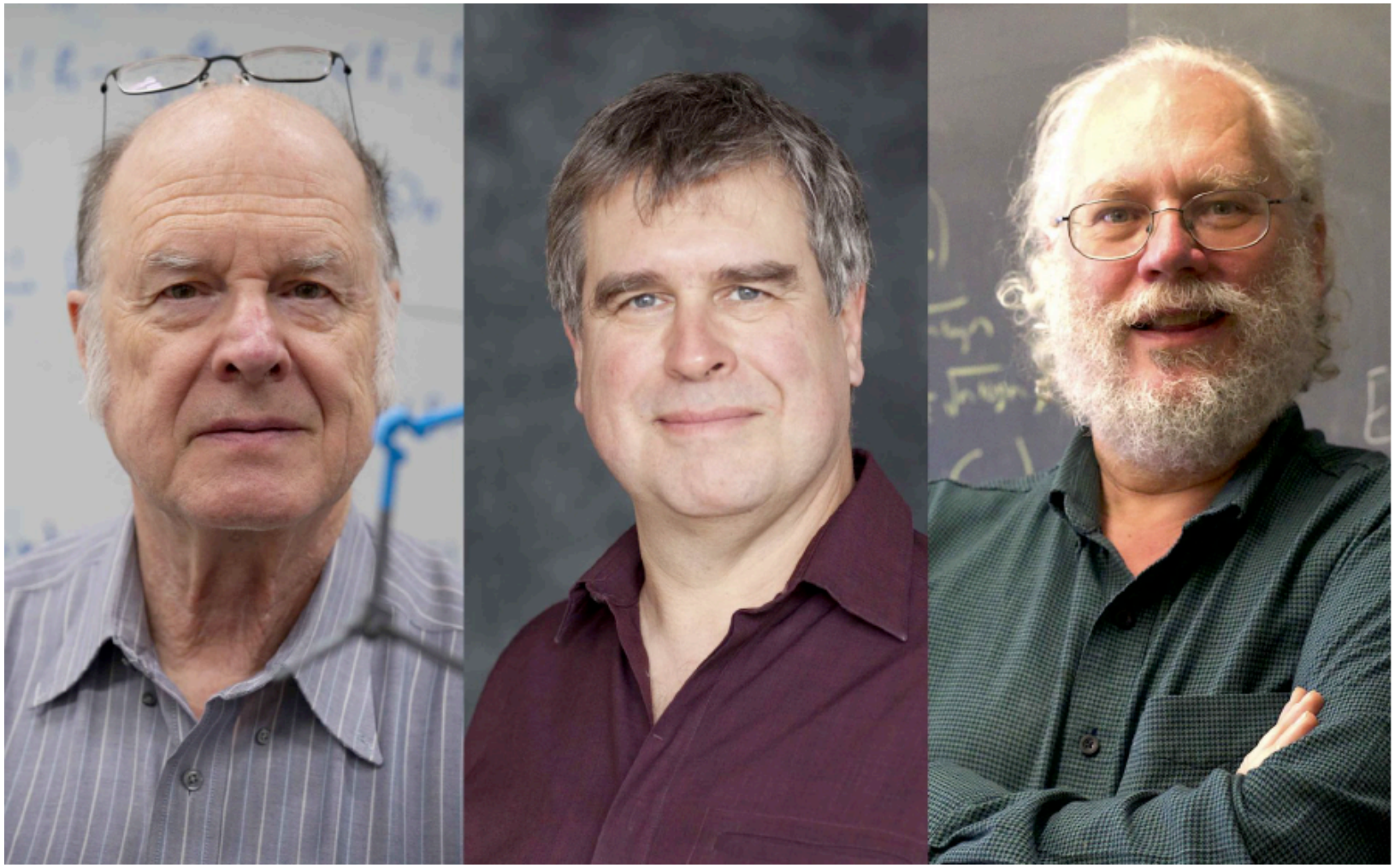
Gilles Brassard 1955

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

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

1984

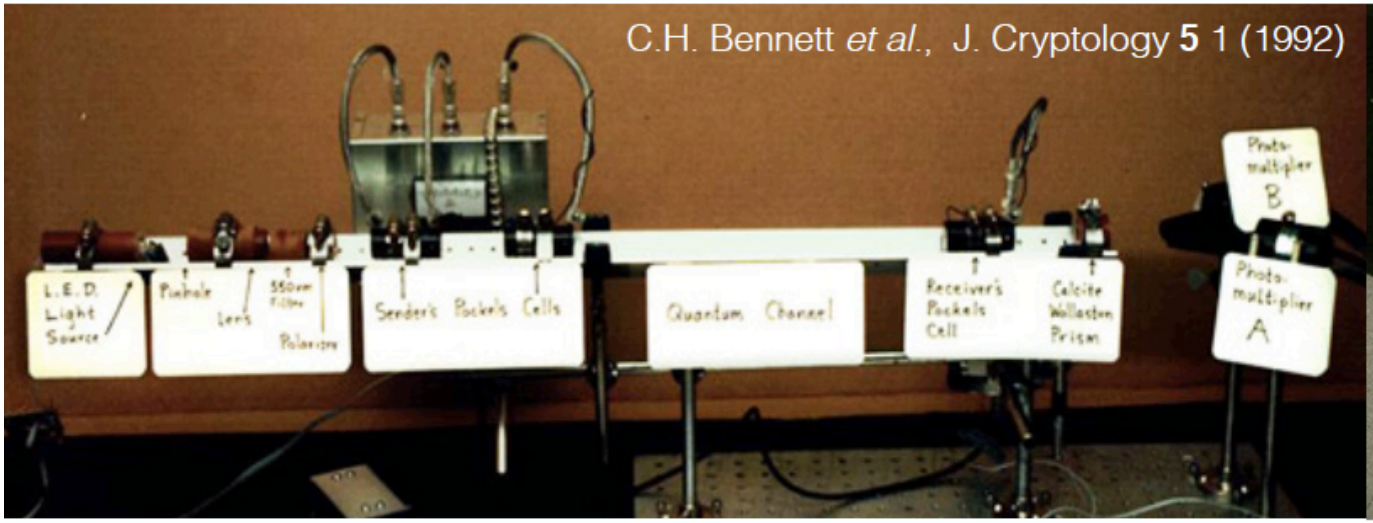
The BBVA prize Frontiers of Knowledge Award in Basic Sciences
to Charles Bennett, Gilles Brassard, and Peter Shor in 2019
for their respective roles in the development of quantum computing
and cryptography

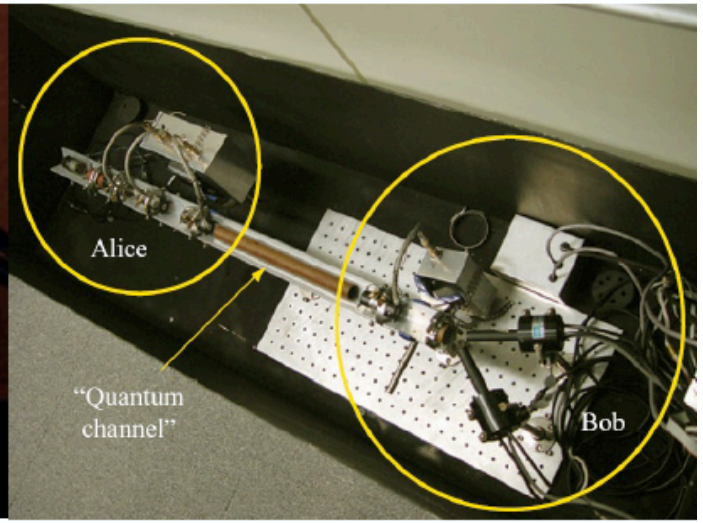


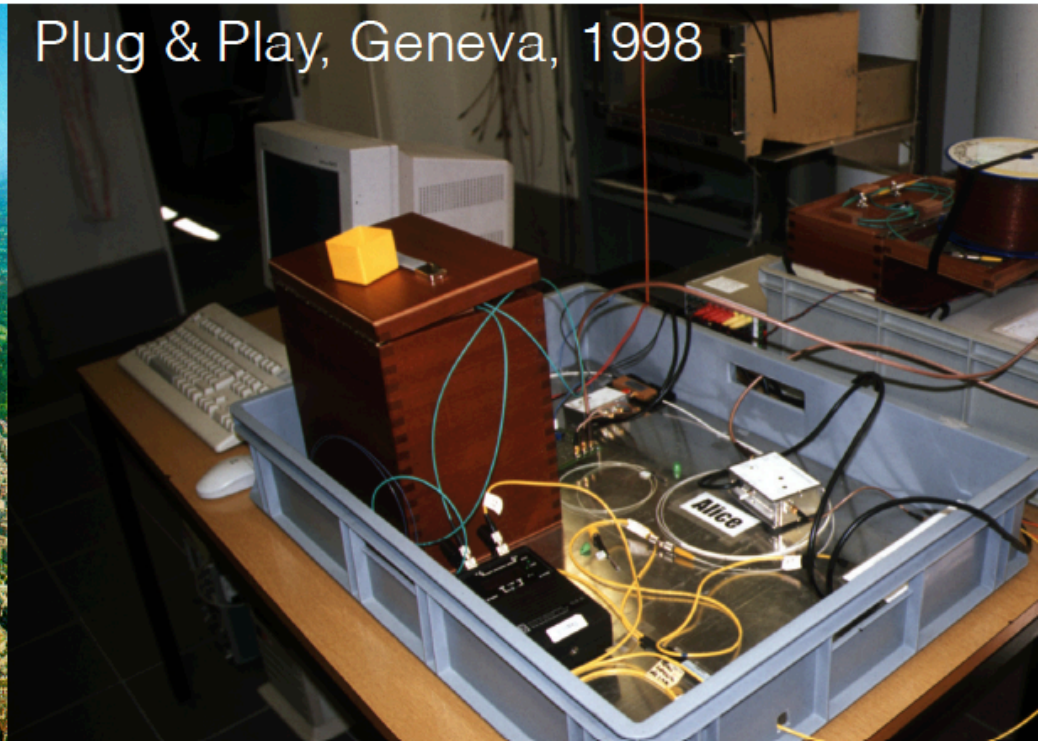
The 19th century was the era of steam power,
the 20th century was the era of information,
and the 21st century will go down in history as the
quantum age, the age in which quantum technologies
dominate all the changes occurring in society, in a way
we cannot yet foresee.”

G. Brassard, 2019

QKD: In the Beginning



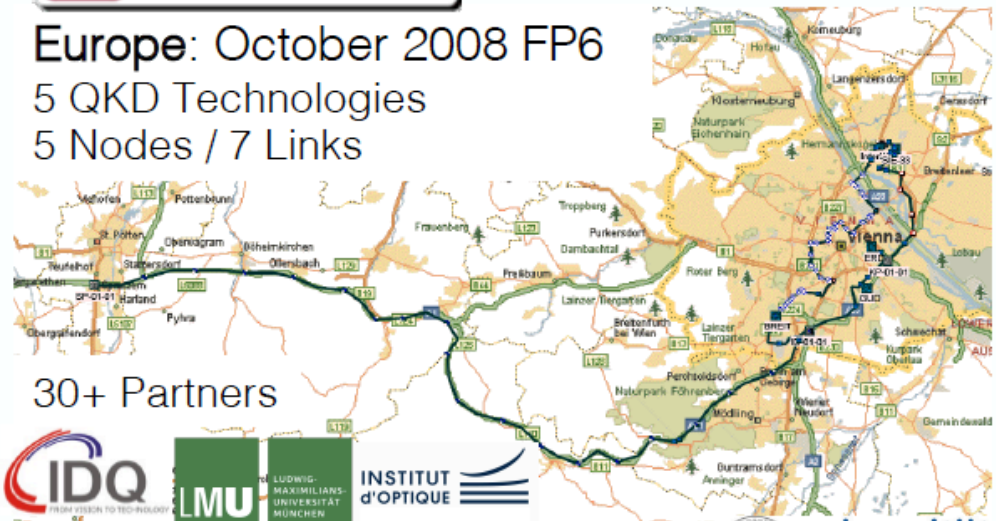




QKD: (Trusted-Node) Networks

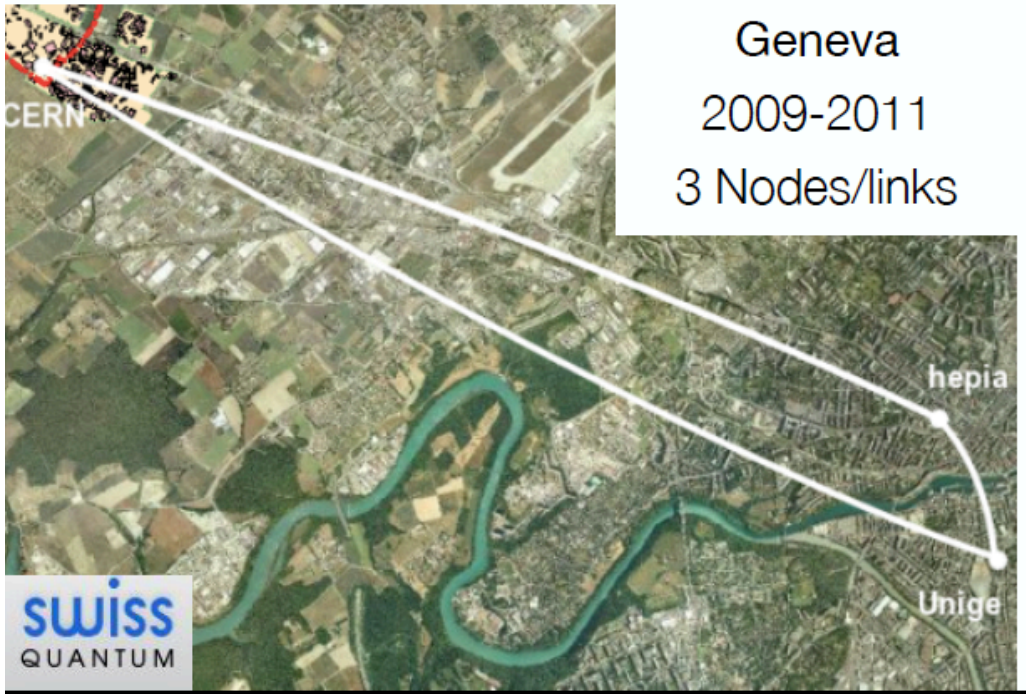
Beating the Distance Limitation

Europe: October 2008 FP6
5 QKD Technologies
5 Nodes / 7 Links

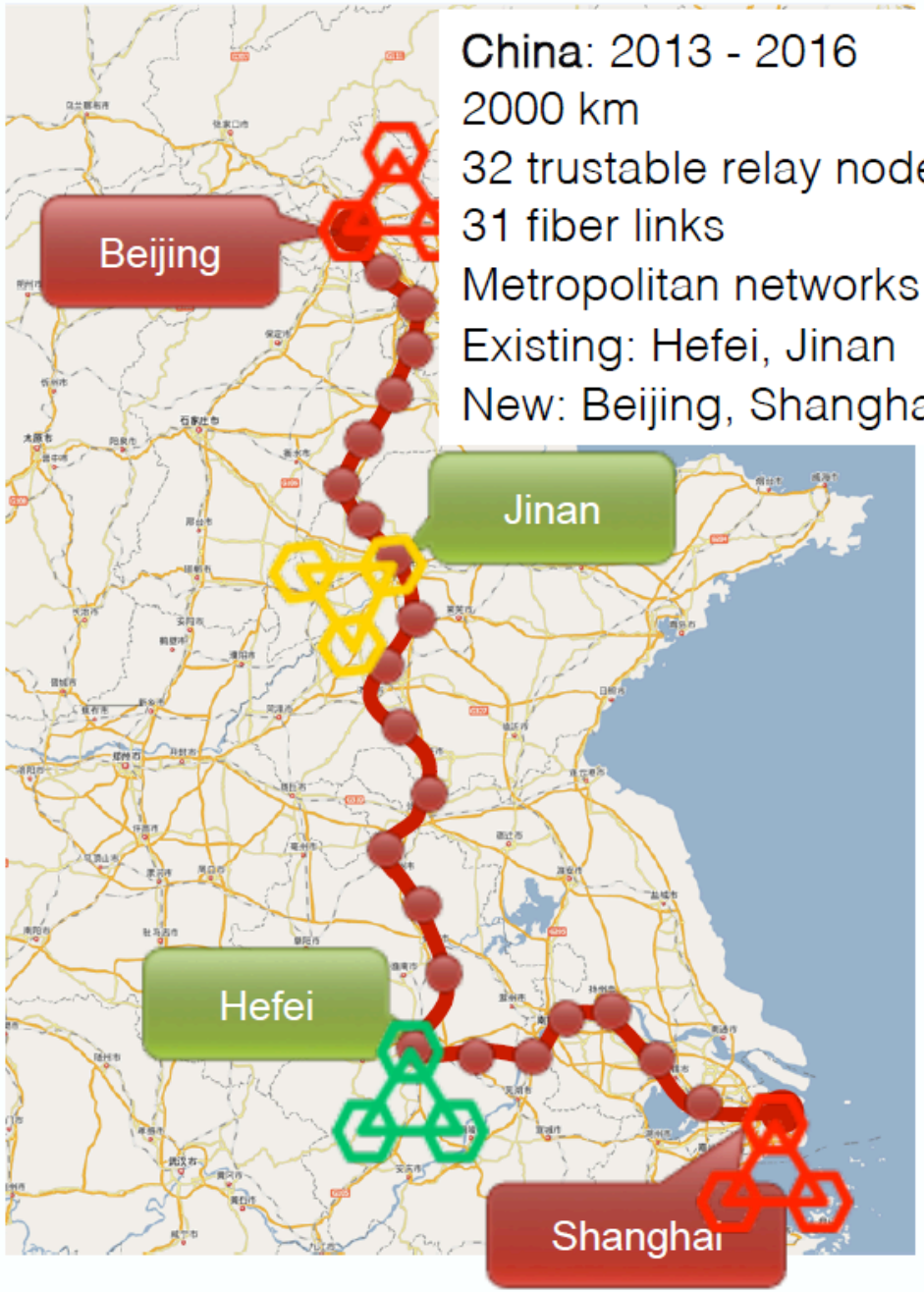


30+ Partners

IDQ · LMU Ludwig-Maximilians-Universität München · Institut d'Optique · Université de Genève · Toshiba · AIT Austrian Institute of Technology · universität wien



Geneva
2009-2011
3 Nodes/links



China: 2013 - 2016
2000 km
32 trustable relay nodes
31 fiber links
Metropolitan networks
Existing: Hefei, Jinan
New: Beijing, Shanghai

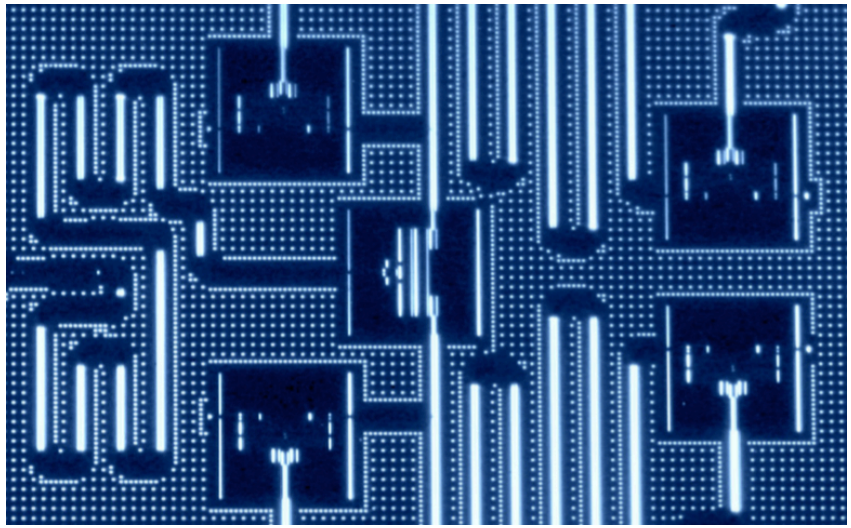
The quantum today

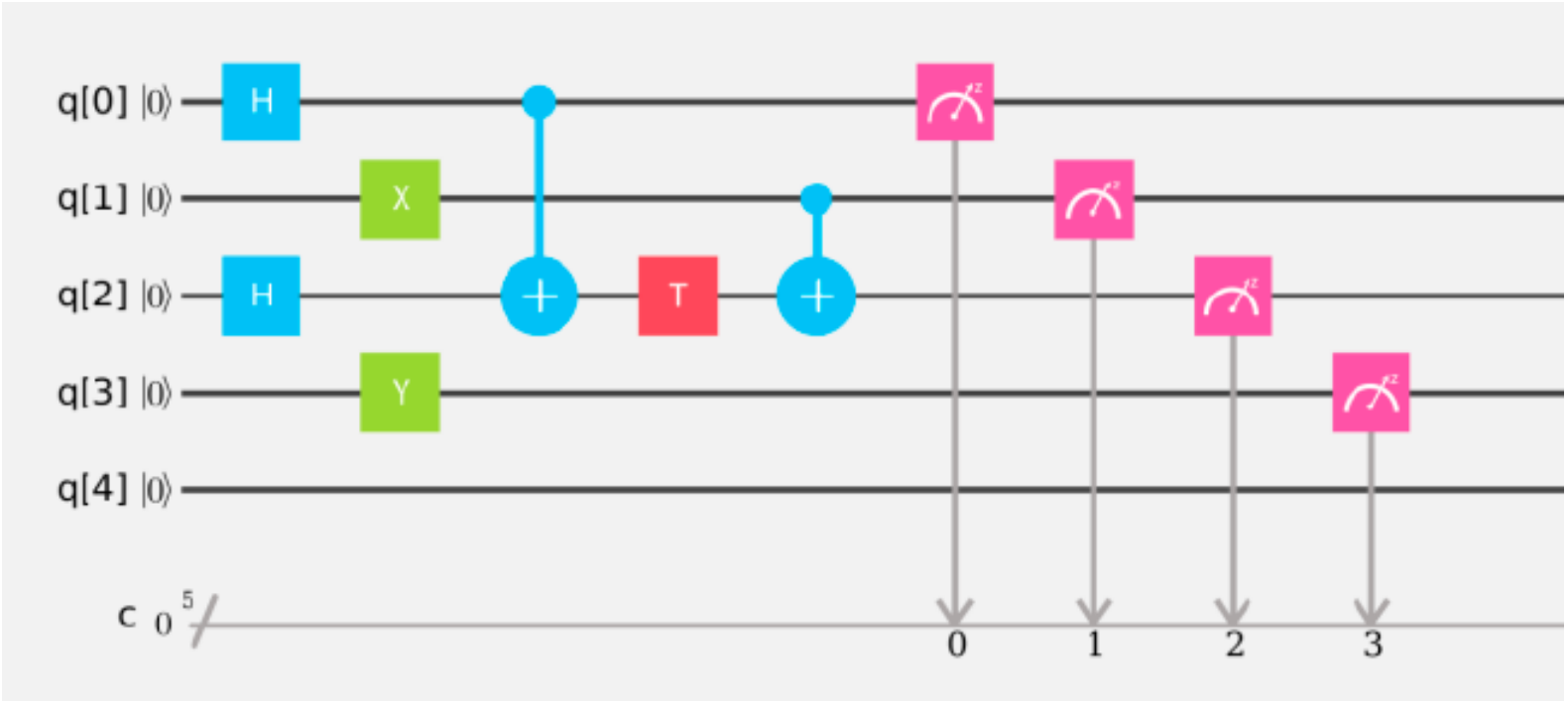
IBM Quantum Experience (2016)

First quantum computer available on the Internet

http://research.ibm.com/ibm-q/

IBM quantum computer of 5 qubits





QUP (Quantum processors) from Wikipedia

Manufa	Name/Codename/Des	Architecture	Fidelity	Qubits	Release date
Google	N/A	Superconducting	99.5%[1]	20 qb	2017
Google	N/A	Superconducting	99.7%[1]	49 qb[2]	Q4 2017 (planned)
Google	Bristlecone	Superconducting	99% (readout) 99.9% (1 qubit) 99.4% (2 qubits)	72 qb[3][4]	5 March 2018
Google	Sycamore	Nonlinear superco	N/A	54 transmon qb 53 qb effective	2019
IBM	IBM Q 5 Tenerife	Superconducting	99.897% (average gate) 98.64% (readout)	5 qb	2016[1]
IBM	IBM Q 5 Yorktown	Superconducting	99.545% (average gate) 94.2% (readout)	5 qb	
IBM	IBM Q 14 Melbourne	Superconducting	99.735% (average gate) 97.13% (readout)	14 qb	
IBM	IBM Q 16 Rüschlikon	Superconducting	99.779% (average gate) 94.24% (readout)	16 qb[5]	17-may-1 (Retired: 26 September 2018)[6]
IBM	IBM Q 17	Superconducting	N/A	17 qb[5]	17-may-1
IBM	IBM Q 20 Tokyo	Superconducting	99.812% (average gate) 93.21% (readout)	20 qb[7]	10 November 2017
IBM	IBM Q 20 Austin	Superconducting	N/A	20 qb	(Retired: 4 July 2018)[6]
IBM	IBM Q 50 prototype	Superconducting	N/A	50 qb[7]	
IBM	IBM Q 53	Superconducting	N/A	53 qb	October 2019
Intel	17-Qubit Superconduc	Superconducting	N/A	17 qb[8][9]	10 October 2017
Intel	Tangle Lake	Superconducting	N/A	49 qb [10]	9 January 2018
Rigetti	8Q Agave	Superconducting	N/A	8 qb	4 June 2018[11]
Rigetti	16Q Aspen-1	Superconducting	N/A	16 qb	30 November 2018[11]
Rigetti	19Q Acorn	Superconducting	N/A	19 qb[12]	17 December 2017
IBM	IBM Armonk[13]	Superconducting	N/A	1 qb	16 October 2019
IBM	IBM Ourense[13]	Superconducting	N/A	5 qb	03 July 2019
IBM	IBM Vigo[13]	Superconducting	N/A	5 qb	03 July 2019
IBM	IBM London[13]	Superconducting	N/A	5 qb	13 September 2019
IBM	IBM Burlington[13]	Superconducting	N/A	5 qb	13 September 2019
IBM	IBM Essex[13]	Superconducting	N/A	5 qb	13 September 2019

Quantum annealers

D-wave: 2.000 qubits. Precio: 15 M$

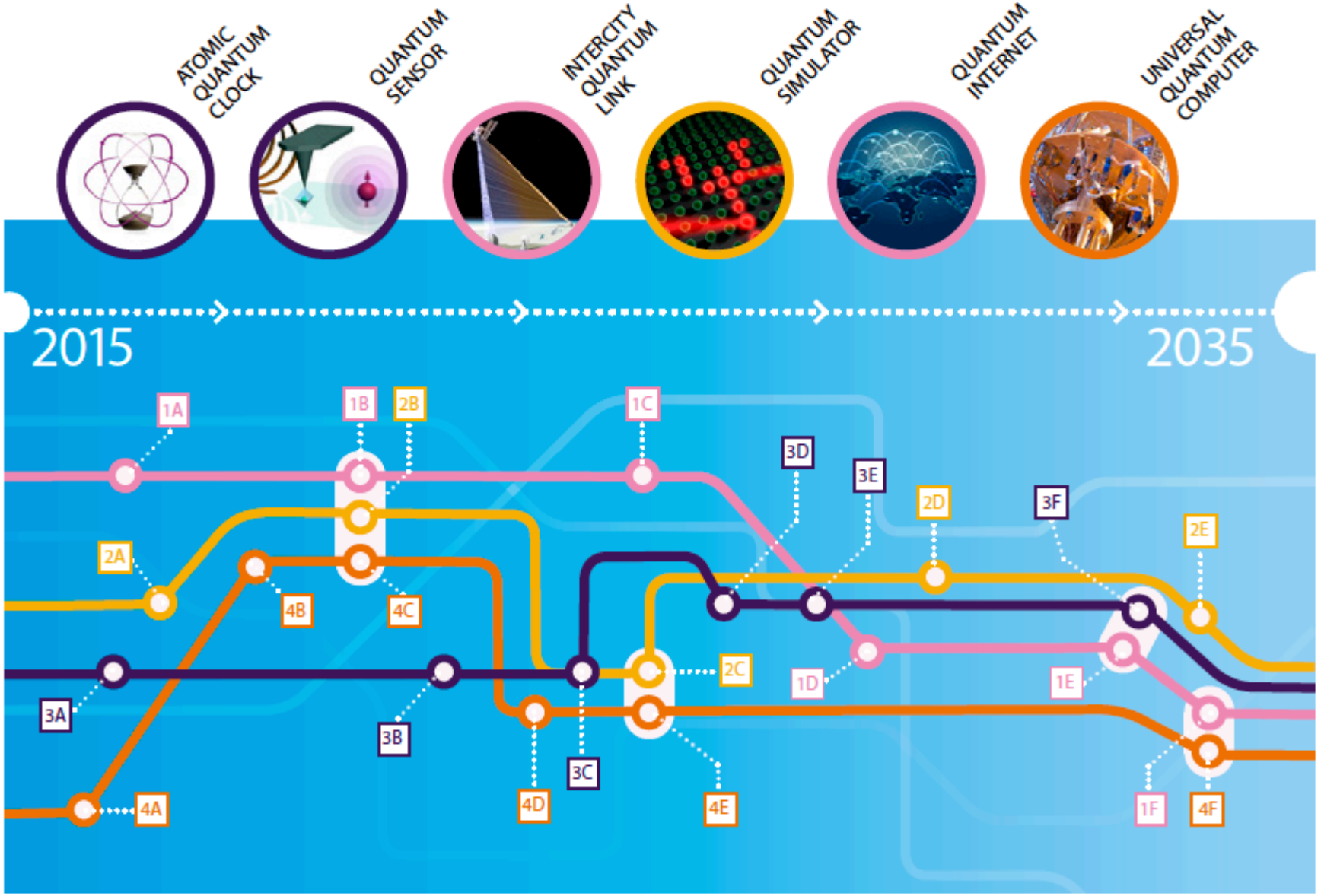
Manufacturer	Name/Codename/Designation	Architecture	Qubits	Release date
D-Wave	D-Wave One (Ranier)	Superconducting	128 qb	11-may-11
D-Wave	D-Wave Two	Superconducting	512 qb	2013
D-Wave	D-Wave 2X	Superconducting	1152 qb	2015
D-Wave	D-Wave 2000Q	Superconducting	2048 qb	2017
D-Wave	D-Wave Advantage	Superconducting	5000 qb	2020

Quantum Manifesto

A New Era of Technology

May 2016

Quantum Technologies Timeline



Questions

The qubit

Definition: a quantum state of a two level system

$|0\rangle, |1\rangle$ basis of computational states $\langle 0|0\rangle = \langle 1|1\rangle = 1, \quad \langle 0|1\rangle = 0$

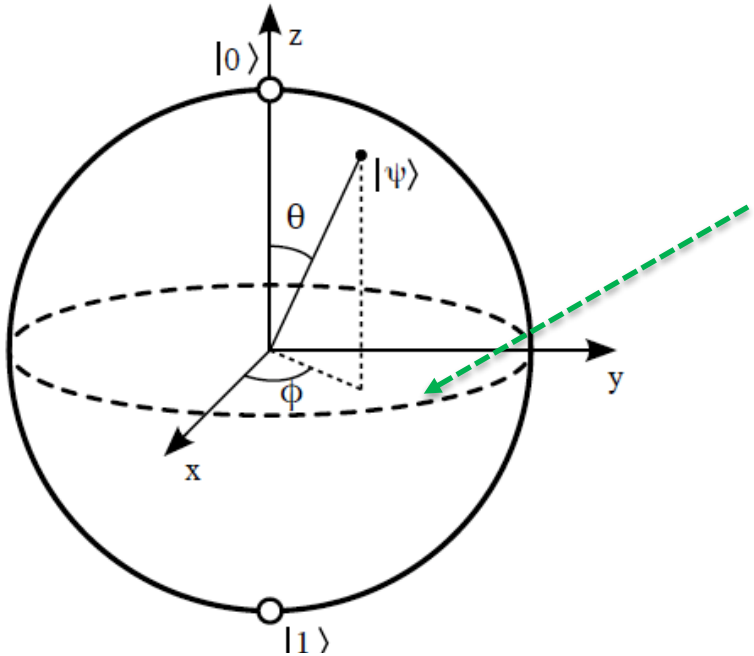
A qubit can be in a pure state or a mixed state

Pure state: $$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \qquad \langle\psi|\psi\rangle = 1$$

$\theta \in [0, \pi]$: polar angle

$\phi \in [0, 2\pi)$: azimuthal angle

Bloch sphere



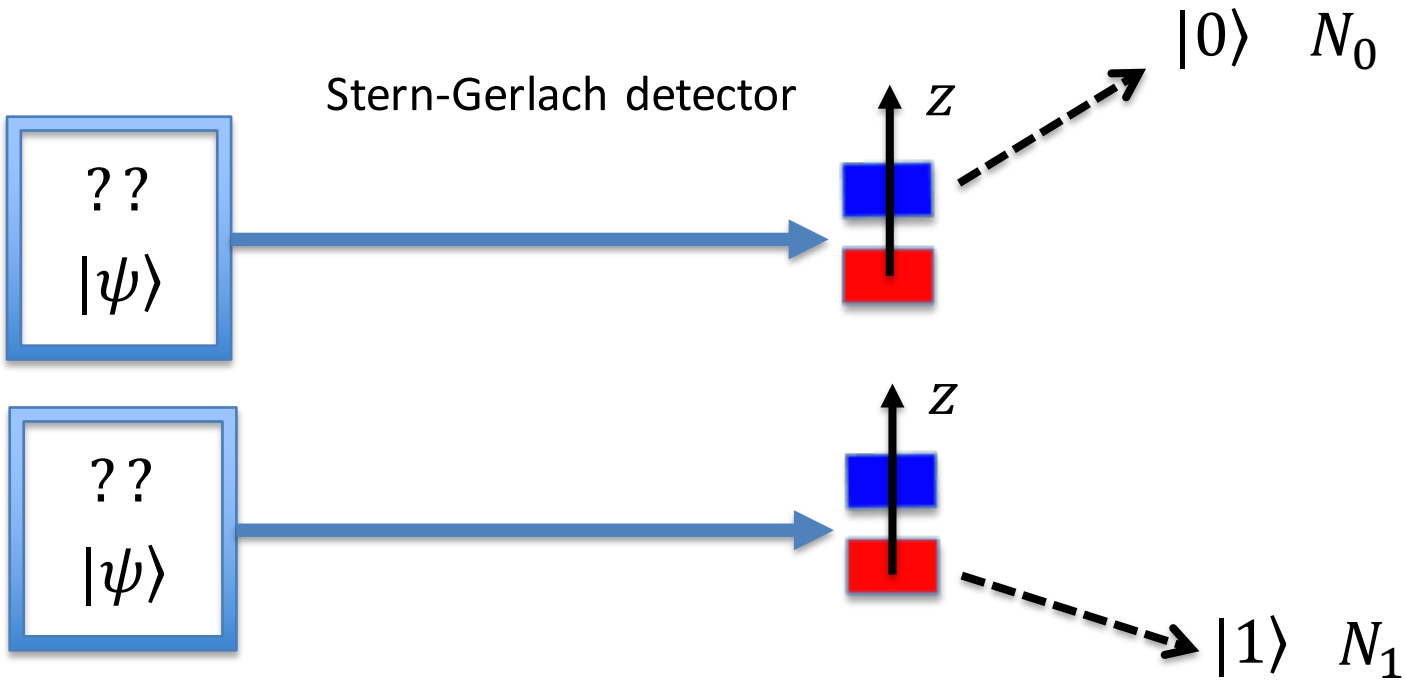
$$\frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}$$

Phys-Math correspondence

Pure state of a qubit ⟺ Point on the Bloch sphere

What is the physical meaning of the angles θ, ϕ ?

Prepare N times an unknown quantum state in the Lab



$$N = N_0 + N_1$$

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

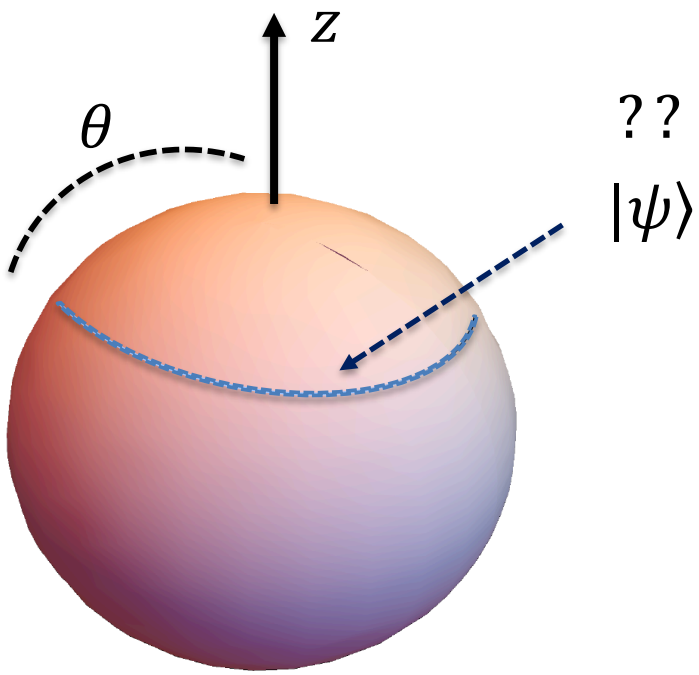
Probability of measuring $|1\rangle$ $\quad p_1 = \dfrac{N_1}{N_0 + N_1}$

$$p_0 + p_1 = 1$$

Quantum Mechanics prediction (Born's law)

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

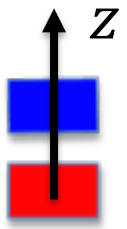
Error $\propto 1/\sqrt{N}$


z
θ
??
|ψ⟩

Vector notation

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

Stern-Gerlach detector



Observable

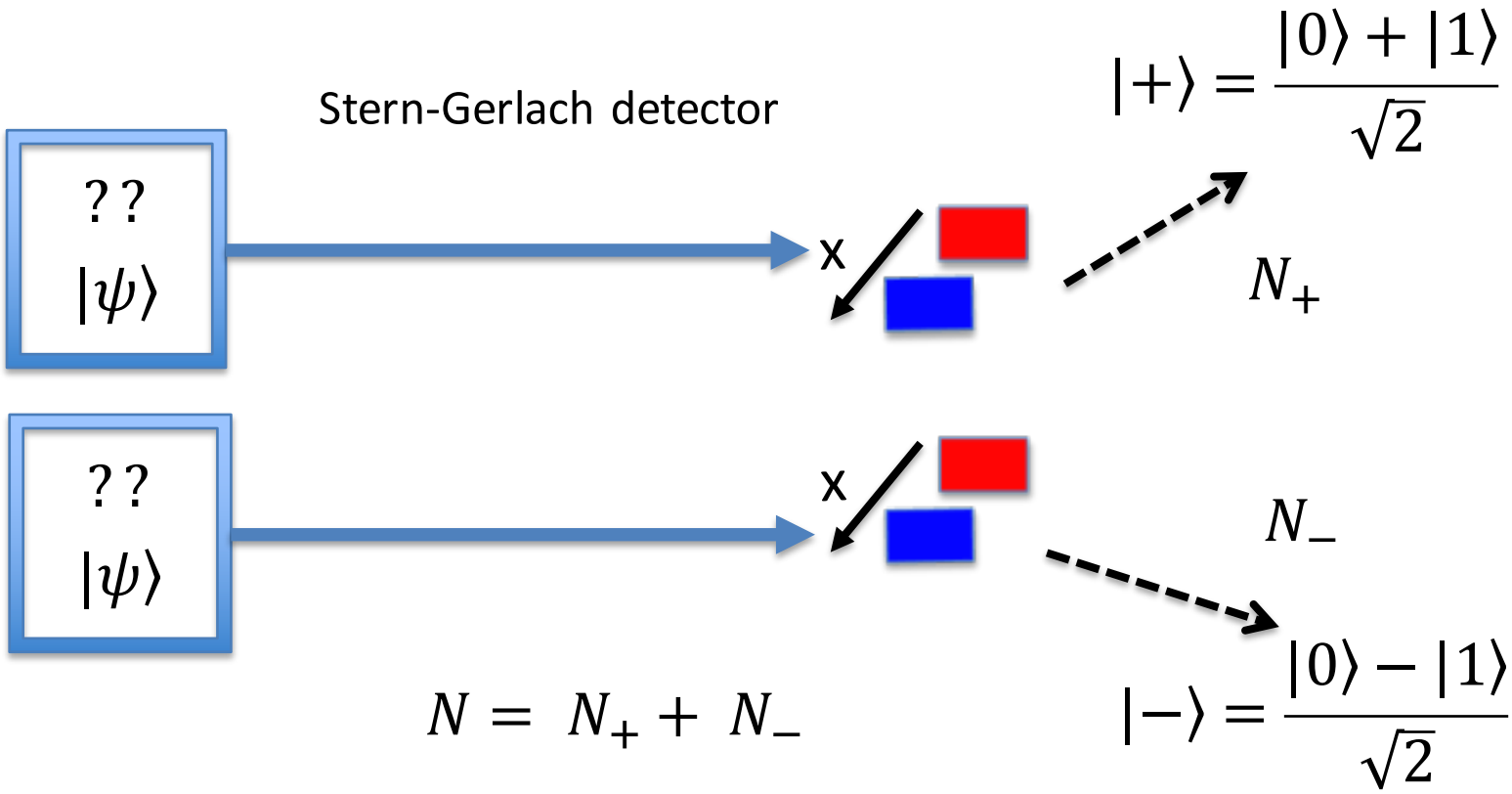
$$\sigma^z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Expectation value

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

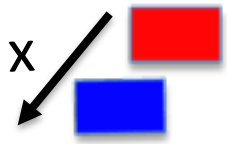
QM $\quad \langle \sigma^z \rangle = \langle \psi | \sigma^z | \psi \rangle = cos^2\frac{\theta}{2} - sin^2\frac{\theta}{2} = \cos\theta$

What about ϕ ?



Stern-Gerlach detector

Observable



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

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

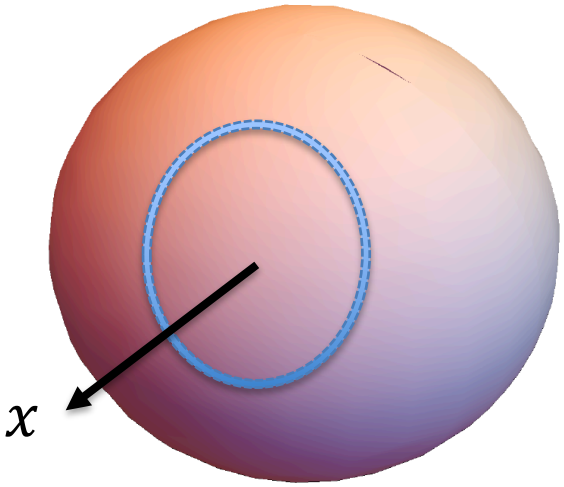
Probability of measuring $|-\rangle$ $\quad p_- = \dfrac{N_-}{N_+ + N_-}$

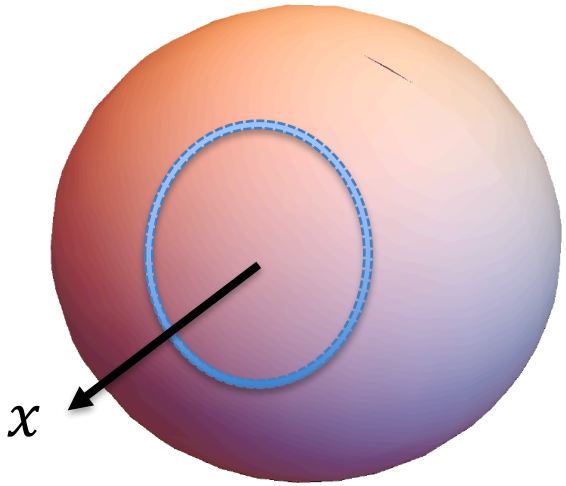
Quantum Mechanics prediction

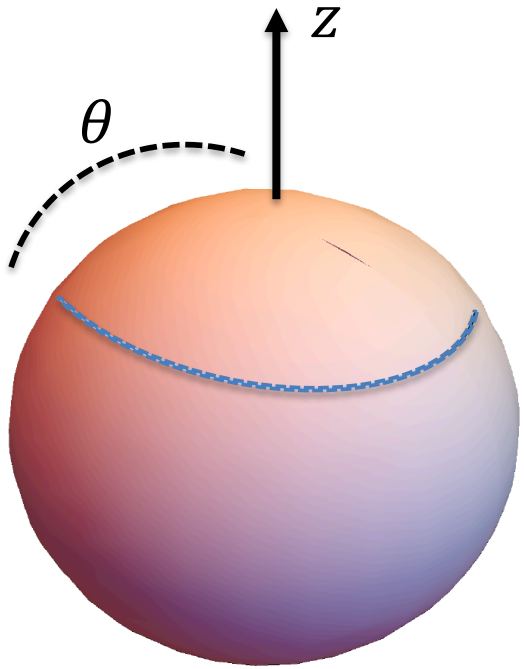
$$p_+ = |\langle +|\psi\rangle|^2 = \frac{1+\sin\theta\cos\phi}{2} \qquad p_- = |\langle -|\psi\rangle|^2 = \frac{1-\sin\theta\cos\phi}{2}$$

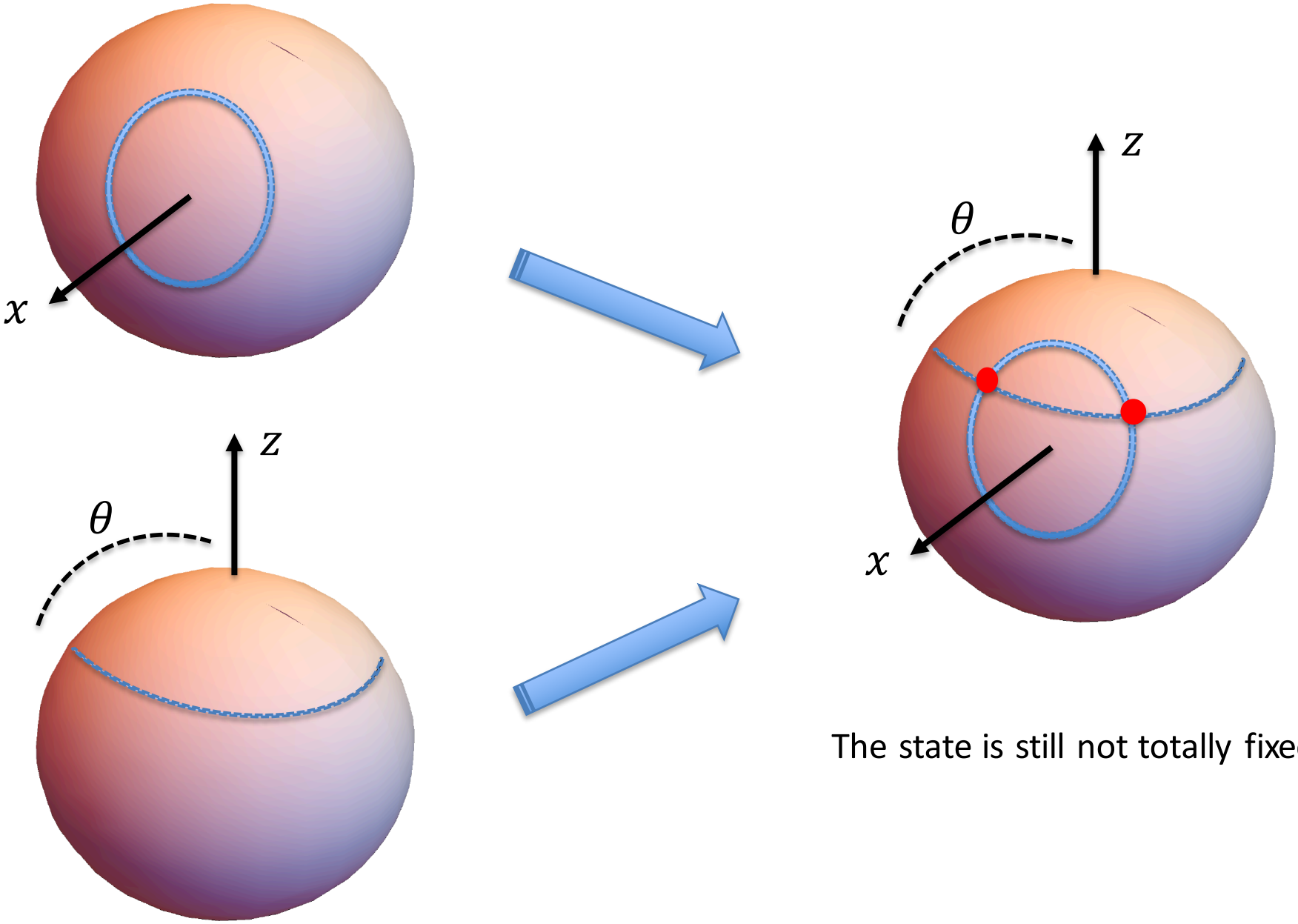
$$\langle\sigma^x\rangle = p_+ - p_-$$

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

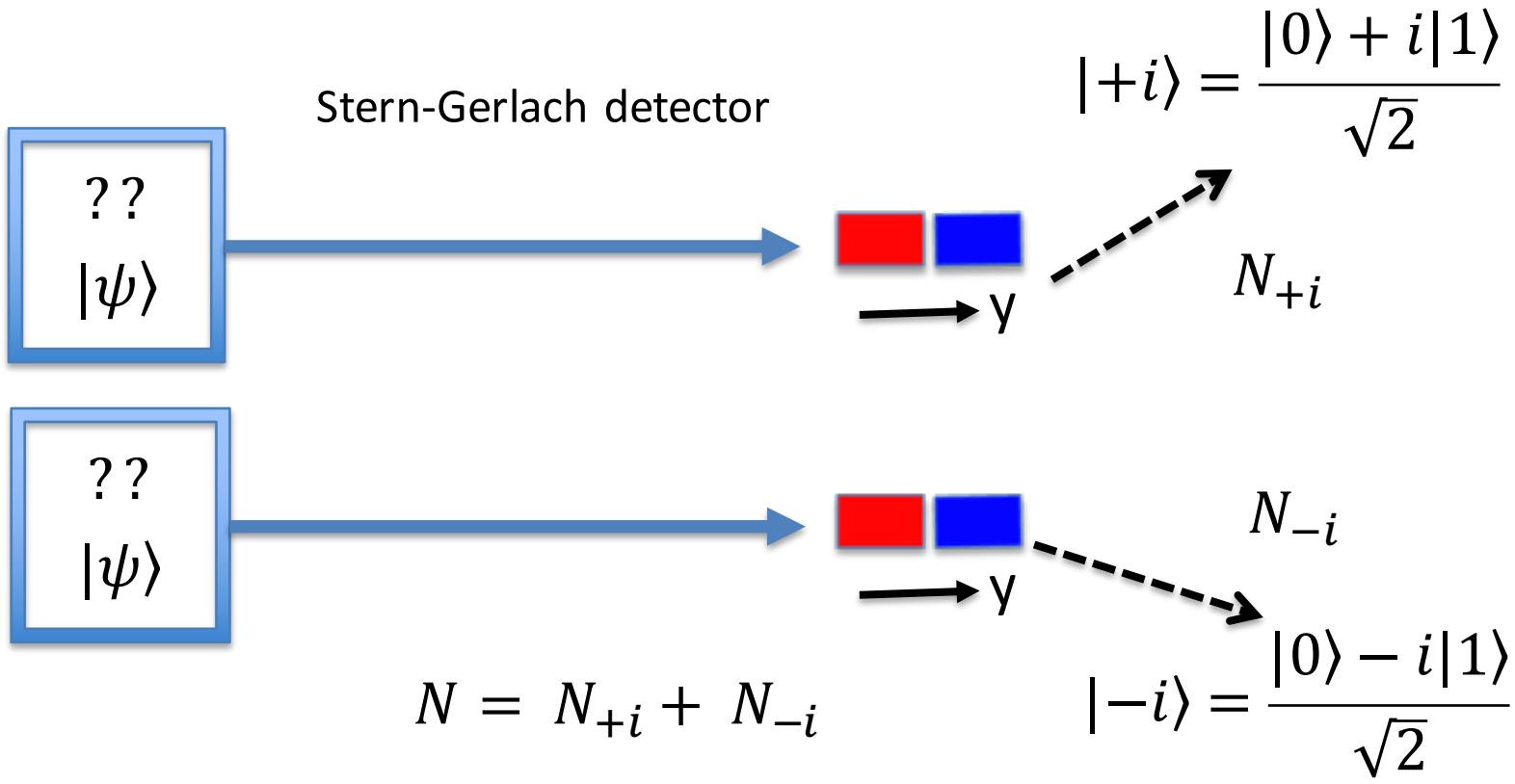

x


x


z
θ



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 $|+i\rangle$ $\quad p_{+i} = \dfrac{N_{+i}}{N_{+i} + N_{-i}}$

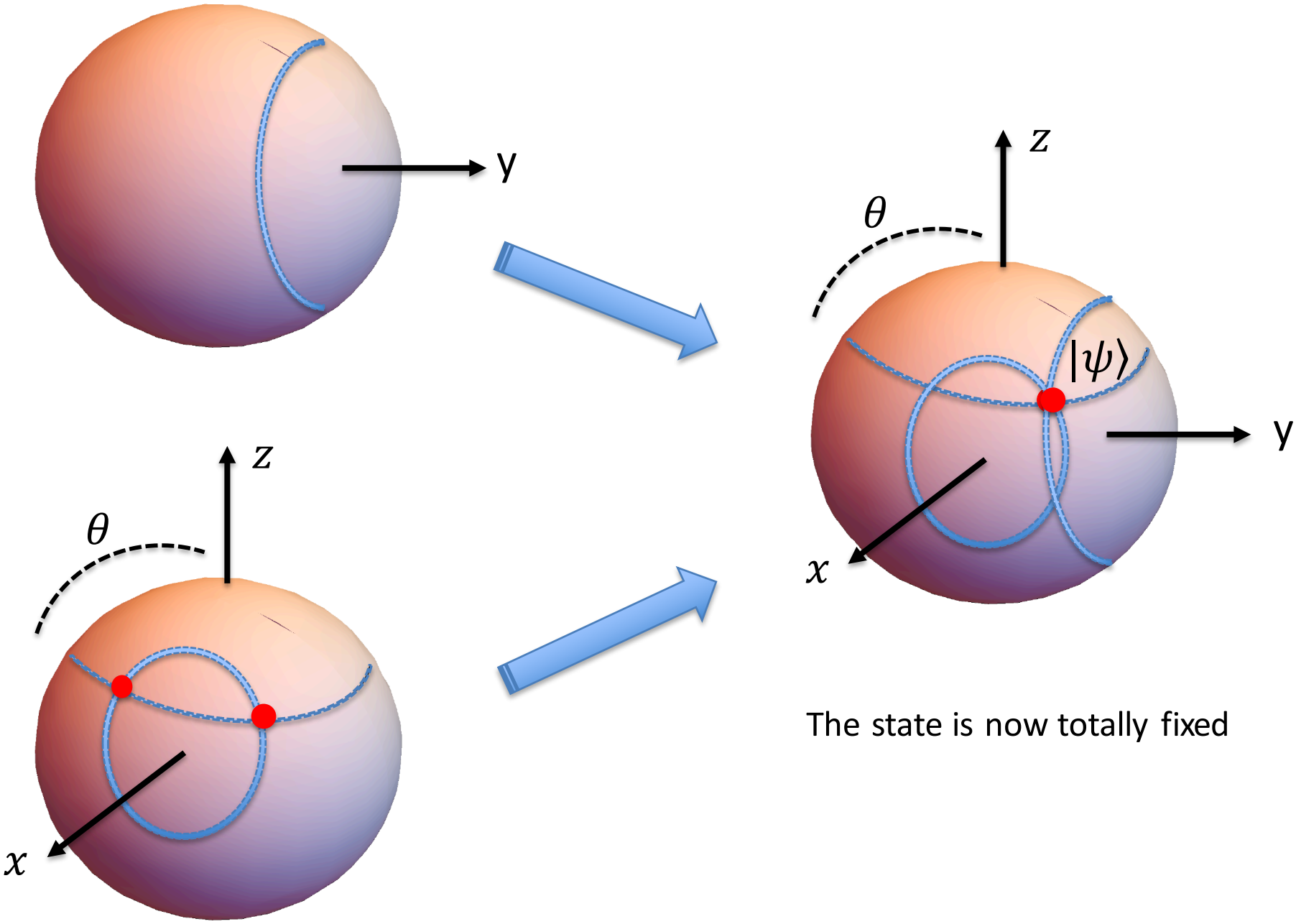
Probability of measuring $|-\rangle$ $\quad p_{-i} = \dfrac{N_{-i}}{N_{+i} + N_{-i}}$

Quantum Mechanics prediction

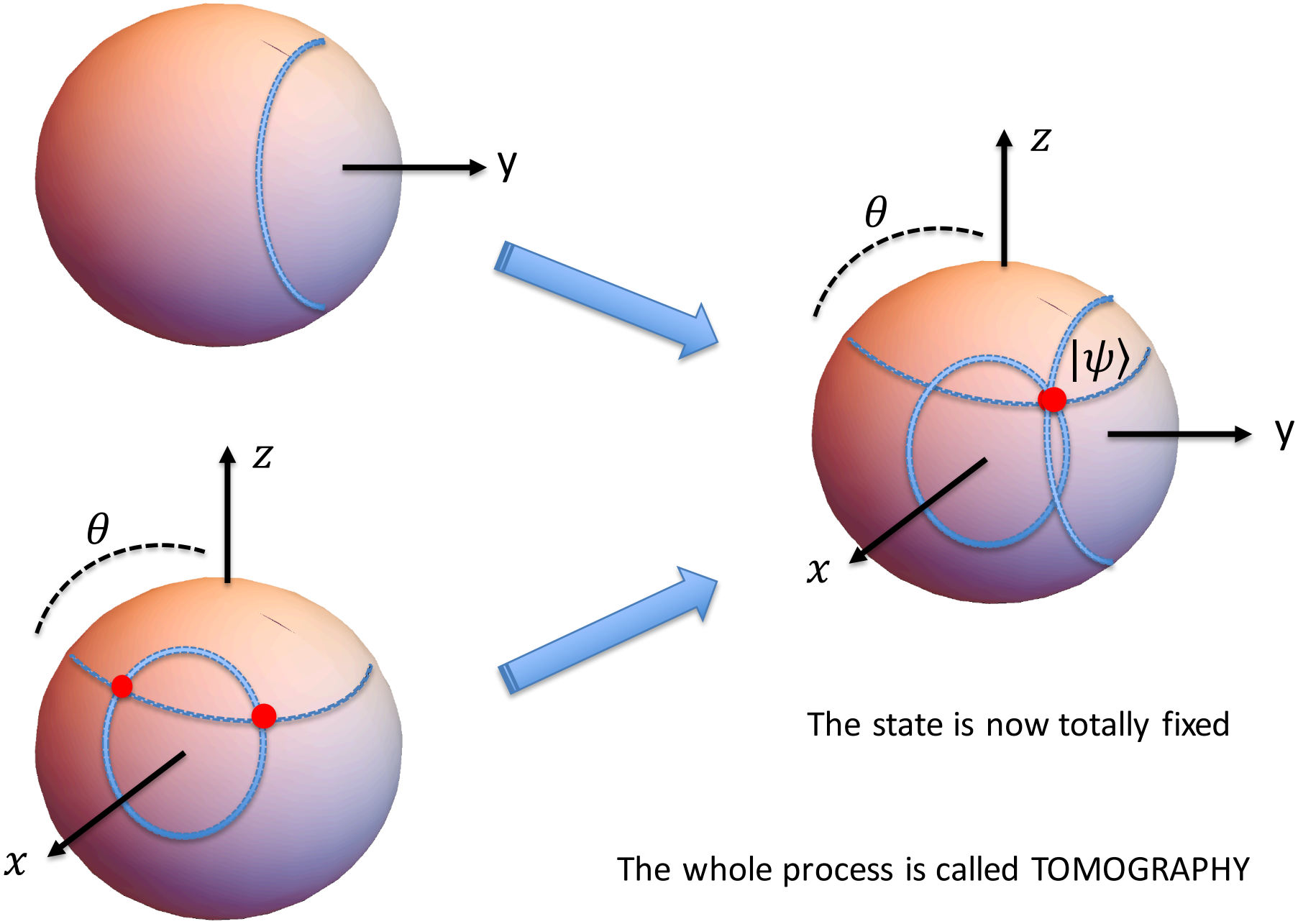
$$p_{+i} = |\langle +i|\psi\rangle|^2 = \frac{1 + \sin\theta \sin\phi}{2} \qquad p_{-i} = |\langle -i|\psi\rangle|^2 = \frac{1 - \sin\theta \sin\phi}{2}$$

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

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



The state is now totally fixed

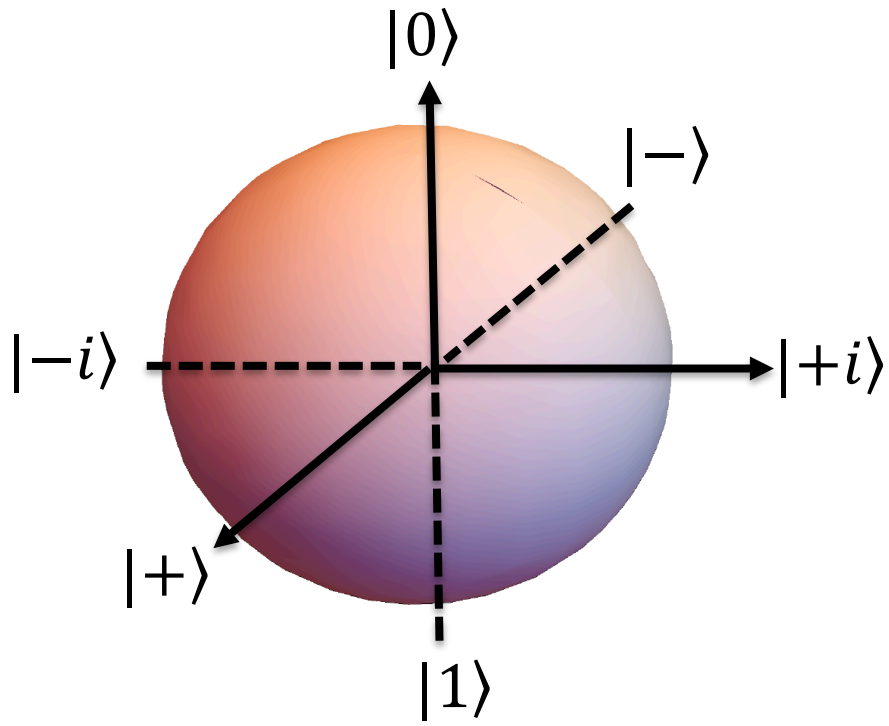


The state is now totally fixed

The whole process is called TOMOGRAPHY

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

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



Density operator

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 operator

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

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

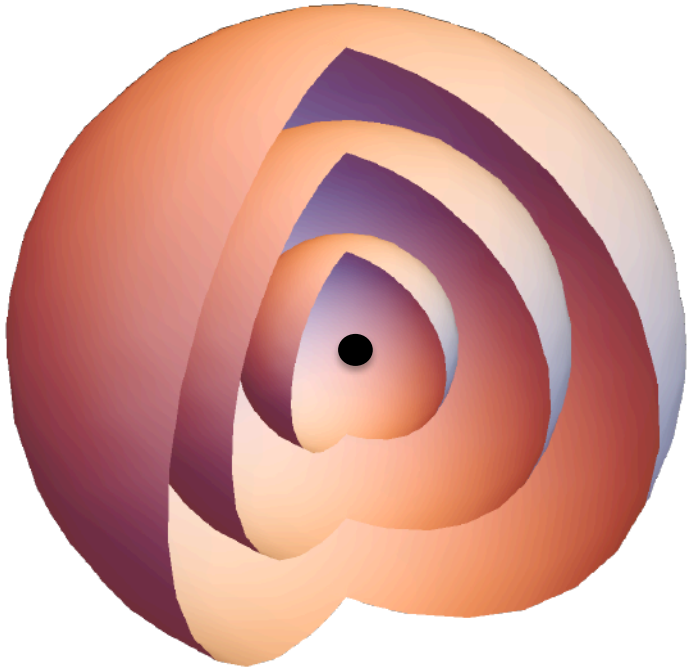
Eigenvalues $\qquad \frac{1+r}{2}, \frac{1-r}{2} \qquad r = \sqrt{x^2 + y^2 + z^2}$

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

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

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

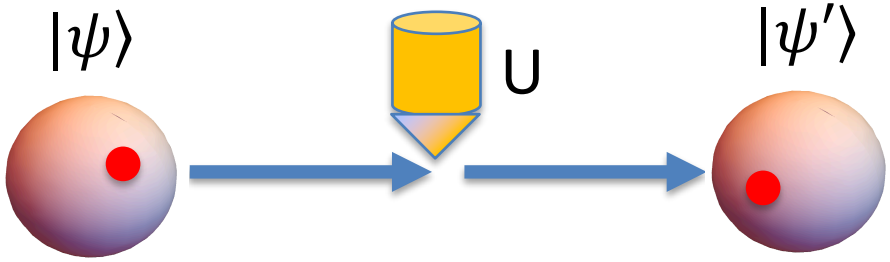
Bloch ball



Questions

Quantum gates

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

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

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

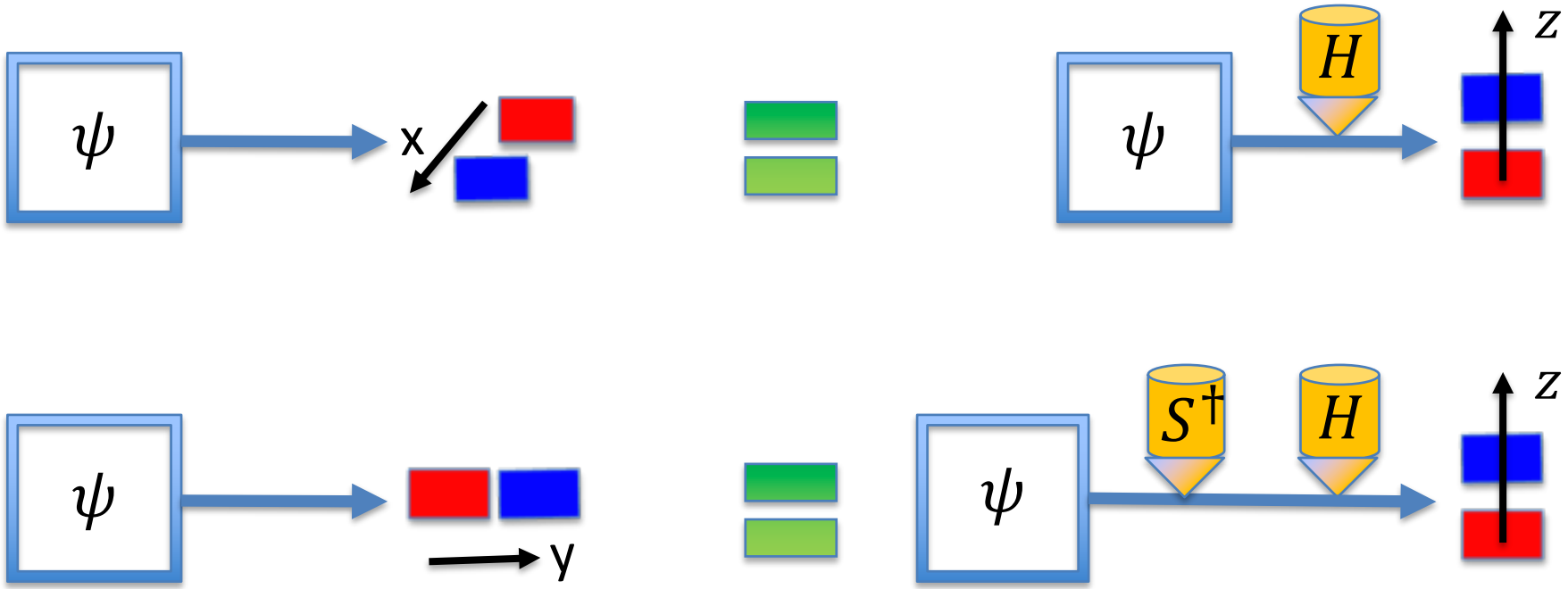
$$\langle Y\rangle_{\psi} = \langle\psi|Y|\psi\rangle = \langle\psi\big|S\,H\,Z\,H\,S^{\dagger}\big|\psi\rangle = \langle Z\rangle_{HS^{\dagger}\psi}$$

Hadamard's magic

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

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

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

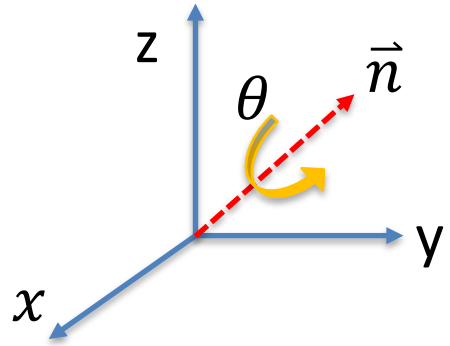


IBM tomography

General qubit gate

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

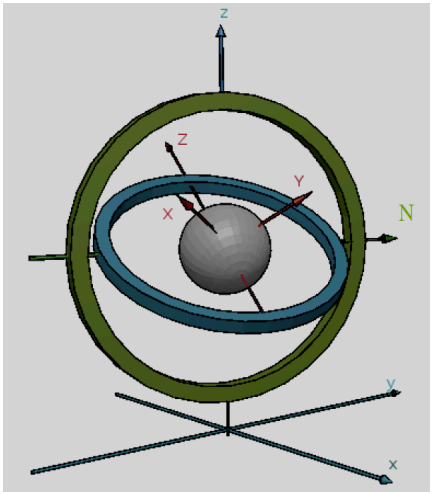
$$R_{\vec{n}}(\theta) = e^{-i\,\theta\vec{n}\cdot\vec{\sigma}/2}$$



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

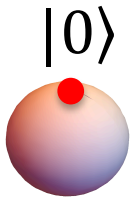
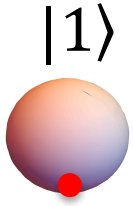
Euler's decomposition $U = e^{i\alpha}R_z(\beta)\,R_y(\gamma)R_z(\delta)$

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



gimbal set

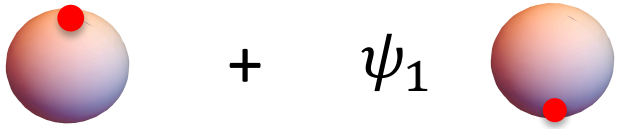
Multiqubit states

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

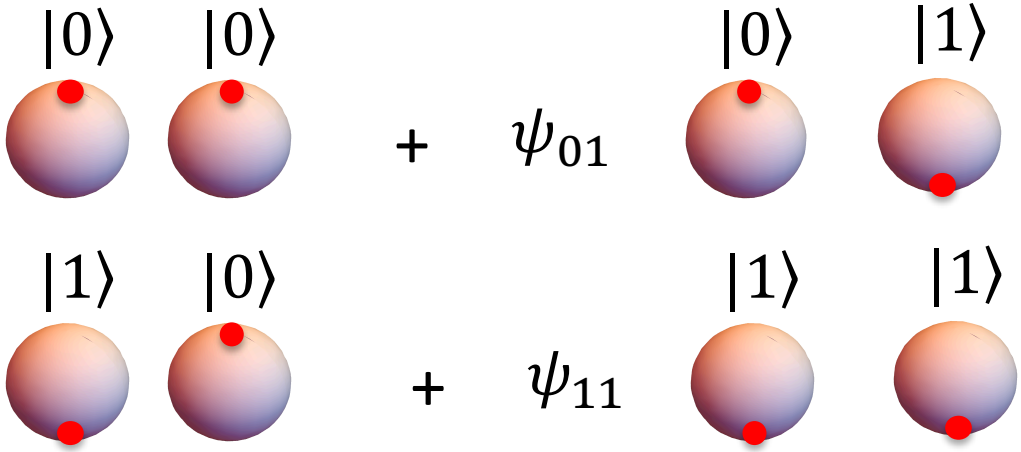
$|0\rangle$ $|1\rangle$

Multiqubit states

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

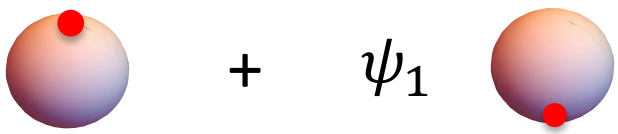


2 qubits $|\psi\rangle = \psi_{00} |0\rangle|0\rangle + \psi_{01} |0\rangle|1\rangle + \psi_{10} |1\rangle|0\rangle + \psi_{11} |1\rangle|1\rangle$

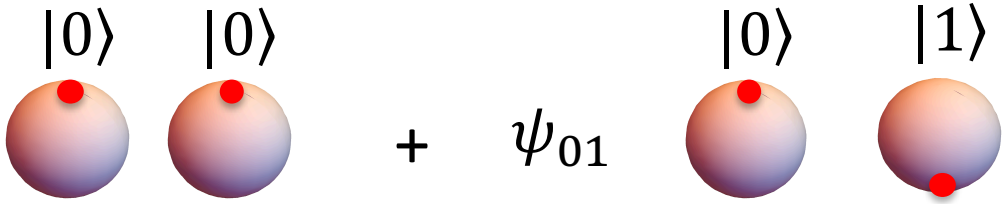


Multiqubit states

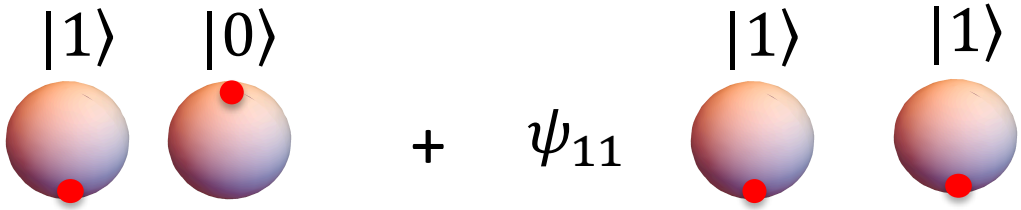
1 qubit $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$



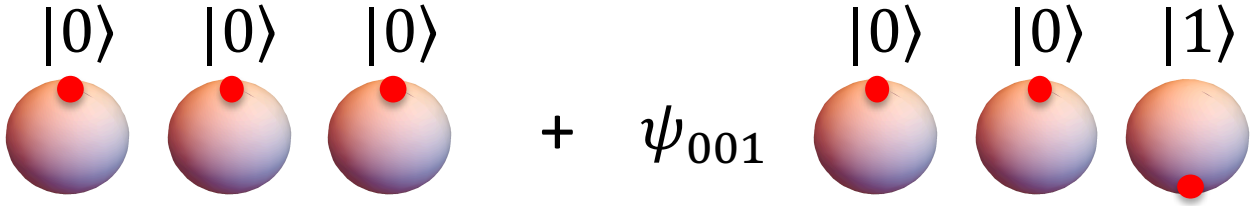
2 qubits $|\psi\rangle = \psi_{00} |0\rangle|0\rangle + \psi_{01} |0\rangle|1\rangle$



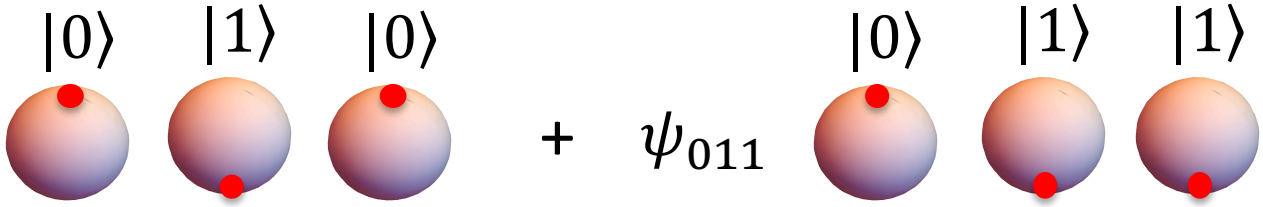
$+ \psi_{10} |1\rangle|0\rangle + \psi_{11} |1\rangle|1\rangle$



3 qubits $|\psi\rangle = \psi_{000} |0\rangle|0\rangle|0\rangle + \psi_{001} |0\rangle|0\rangle|1\rangle$



$+ \psi_{010} |0\rangle|1\rangle|0\rangle + \psi_{011} |0\rangle|1\rangle|1\rangle$



$+$

4 terms

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

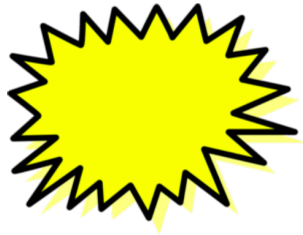
Entangled states

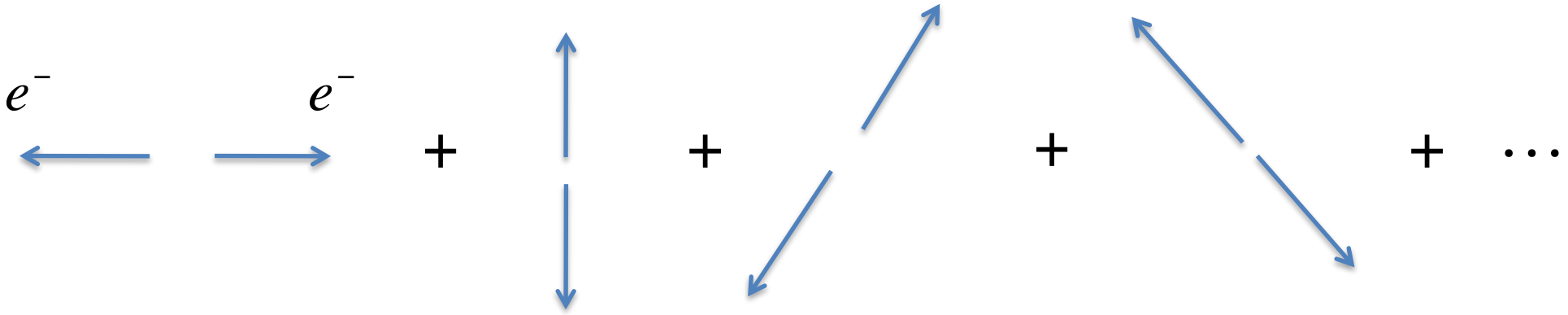
$$|\psi\rangle = \psi_{00}\,|0\rangle\,|0\rangle + \psi_{01}\,|0\rangle\,|1\rangle + \psi_{10}\,|1\rangle\,|0\rangle + \psi_{11}\,|1\rangle\,|1\rangle$$

$$\neq$$

$$\left(\chi_0\,|0\rangle + \chi_1\,|1\rangle\right) \times \left(\zeta_0\,|0\rangle + \zeta_1\,|1\rangle\right)$$

EPR state : Gedanken experiment





Linear superposition of two electrons with opposite momentum

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 entangled in each of these states

Used in the teleportation protocol

Two qubit gates

CNOT = Controlled NOT

control qbit

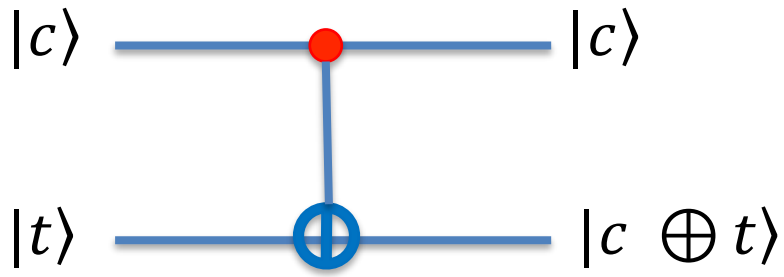
target qbit

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

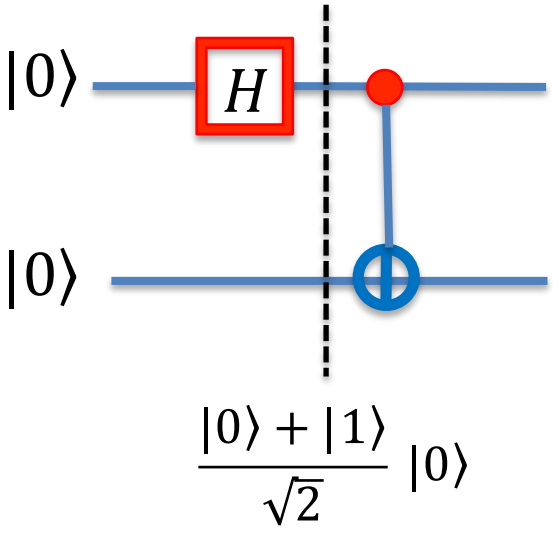
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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

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

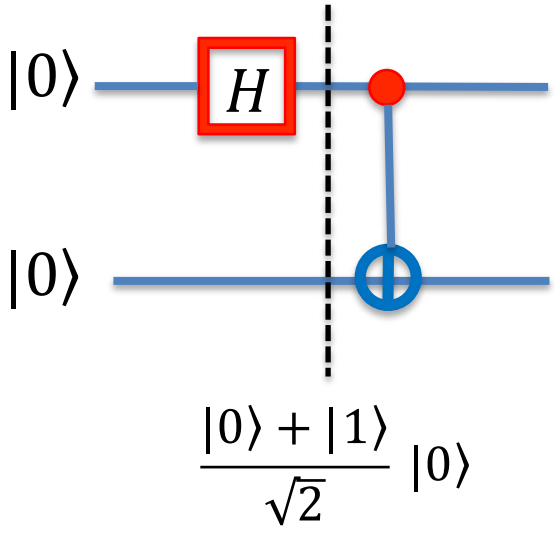


Creation of entanglement

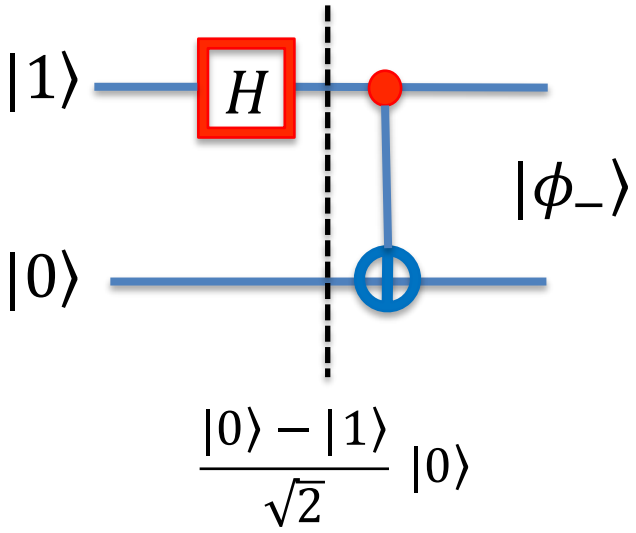


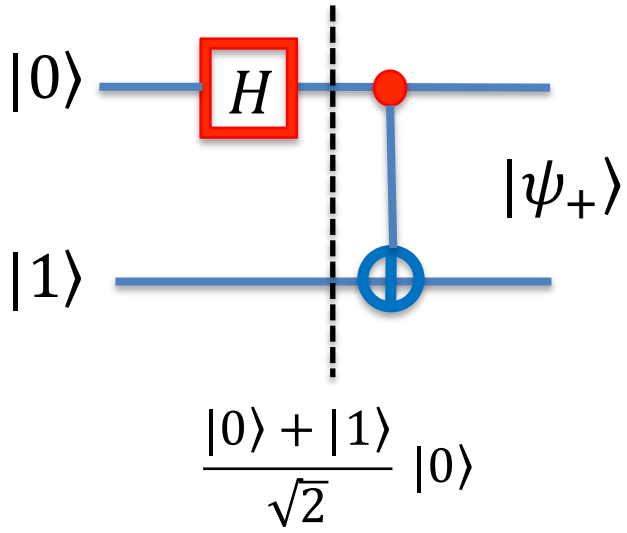
$$|\phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

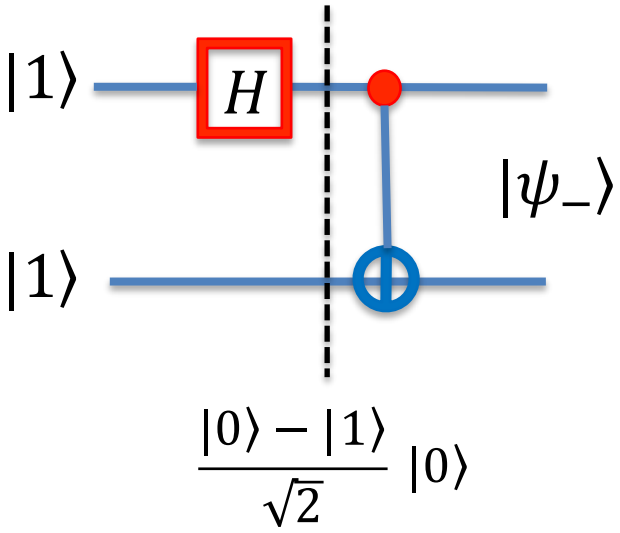
Creation of entanglement



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

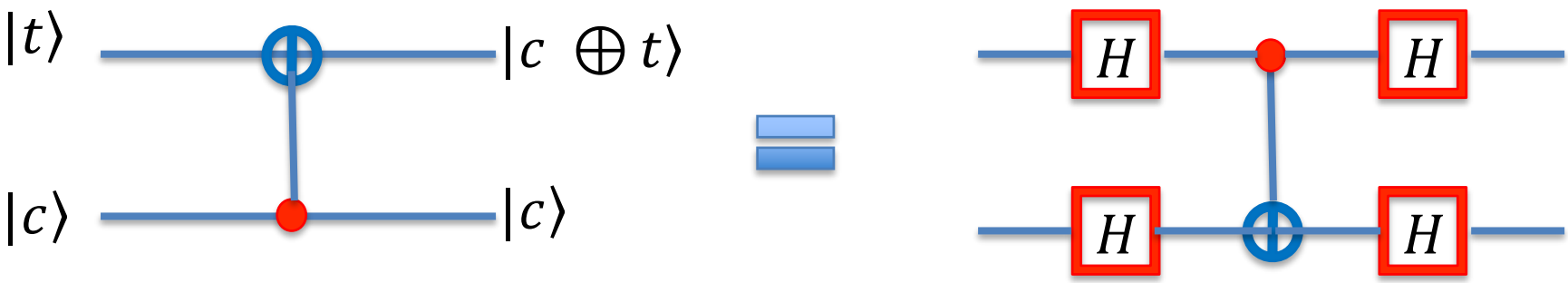






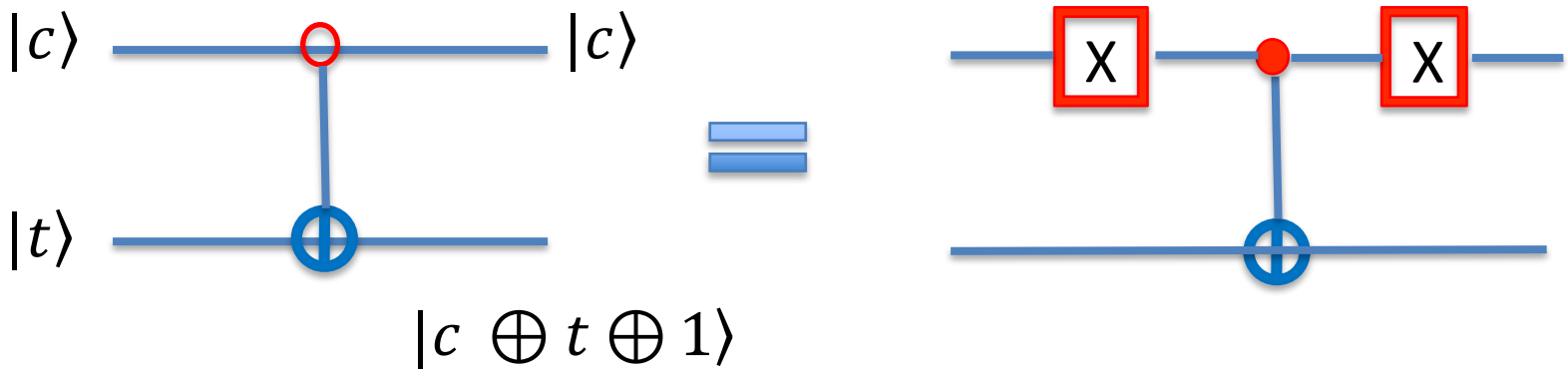
Computational basis -> Bell basis

Changing roles



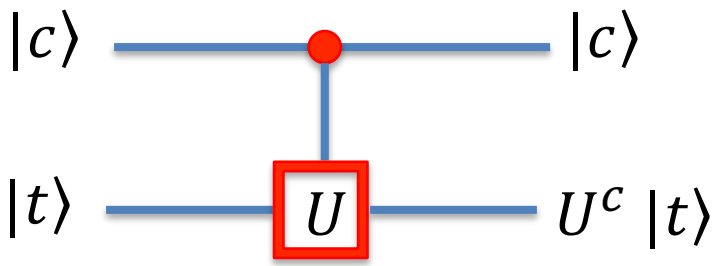
When the control is 0 not 1

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



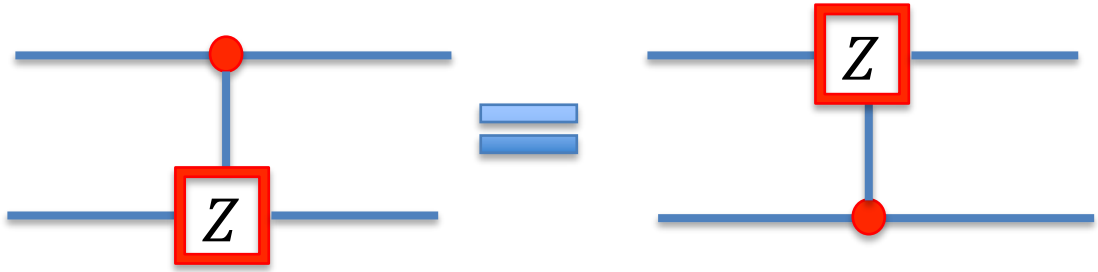
General Control

$CU =$



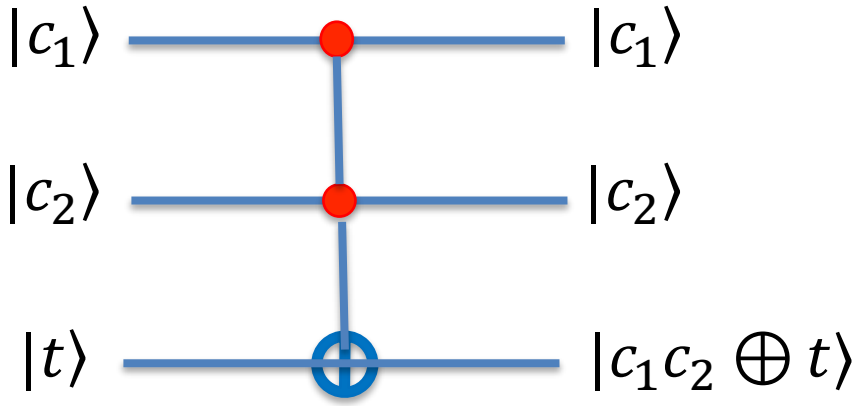
CNOT $= CX$

$CZ =$

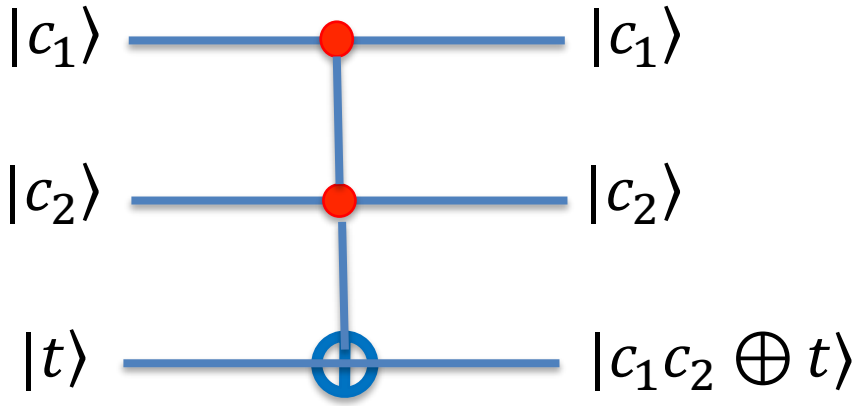


$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

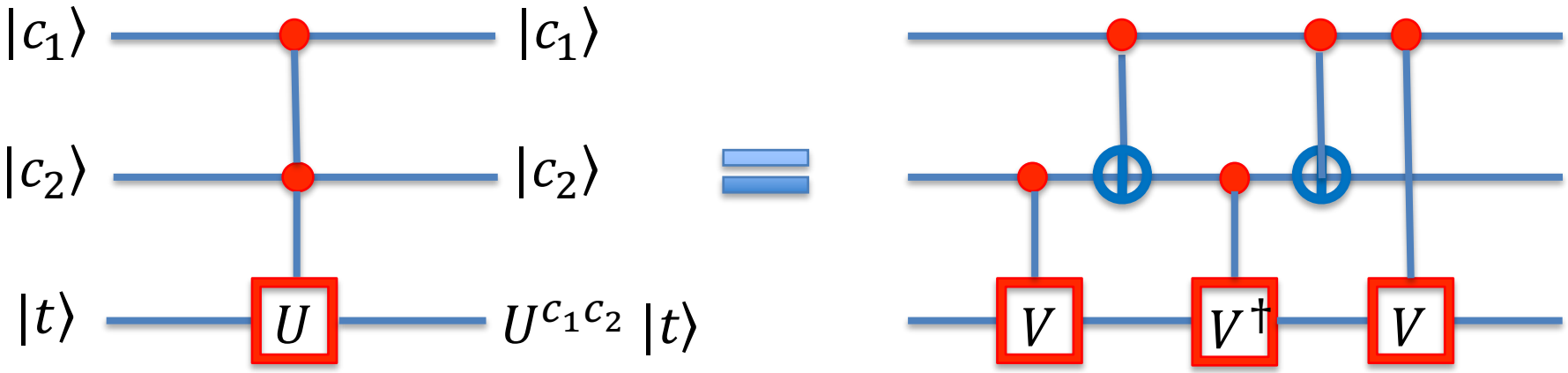
Toffoli gate = CCNOT



Toffoli gate = CCNOT



Generalized Toffoli gate = CCU



$$U = V^2$$

Standard Toffoli $\quad U = X, V = (1-i)(\mathbb{I} + i\,X)/2$

Universal classical gates

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

Non reversible: AND, OR, NOT

Reversible: Toffoli

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

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

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

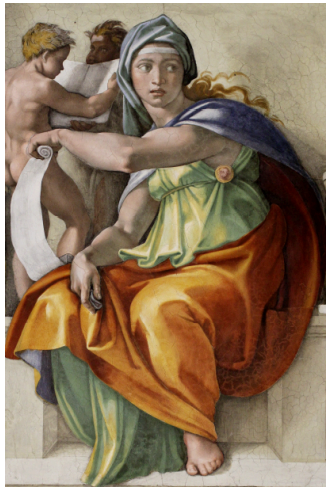
Constant function: $f(0) = f(1)$ $\qquad$ Balanced function: $f(0) \neq f(1)$

f_0 , f_3 $\qquad$ 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 process is denoted as “calling TWICE an oracle”

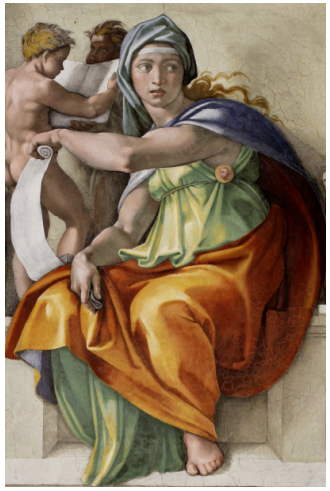


Delphi oracle

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

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

This process is denoted as “calling TWICE an oracle”

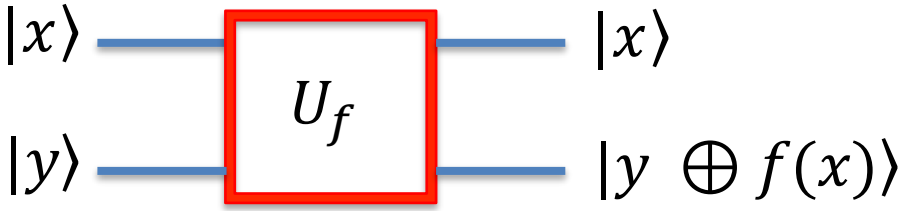


Delphi oracle

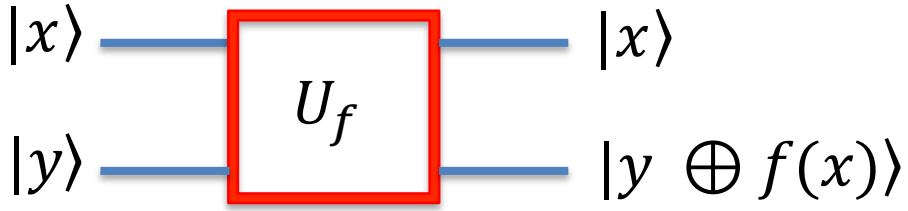
Question: Can one call only ONCE the oracle ?

Answer: YES using quantum parallelism and interference

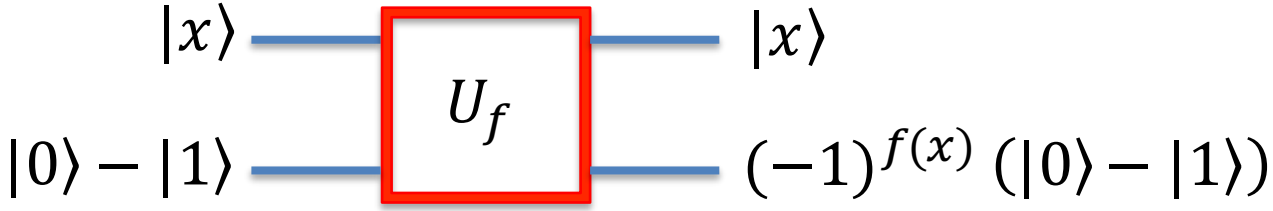
Quantum oracle



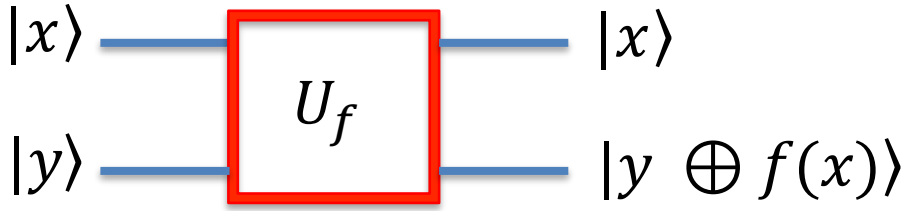
Quantum oracle



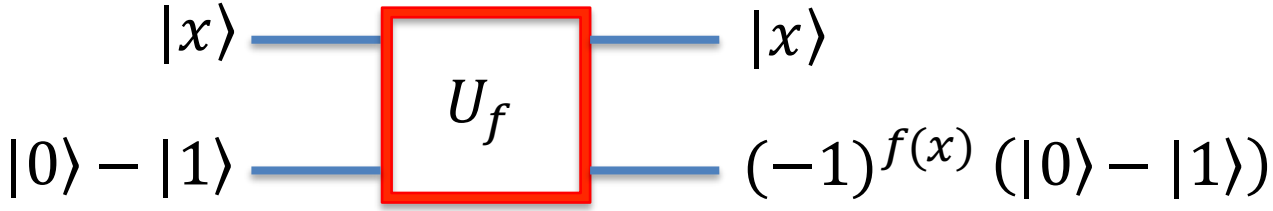
Step 1: call to the oracle



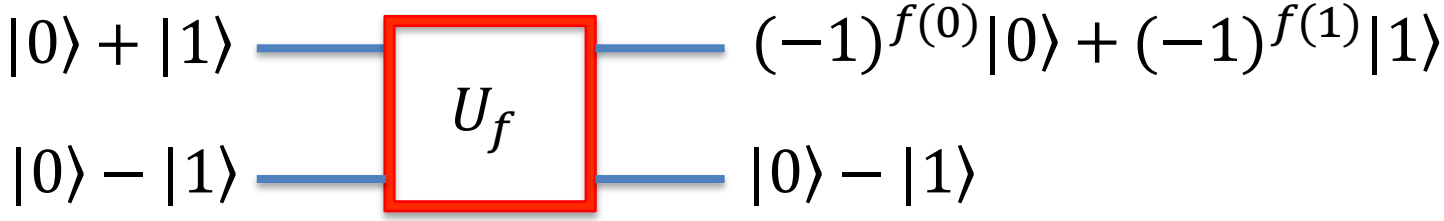
Quantum oracle



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

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

Step 4: getting the answer

If $f(0) = f(1)$ → $|0\rangle$

If $f(0) \neq f(1)$ → $|1\rangle$

Step 3: quantum data mining

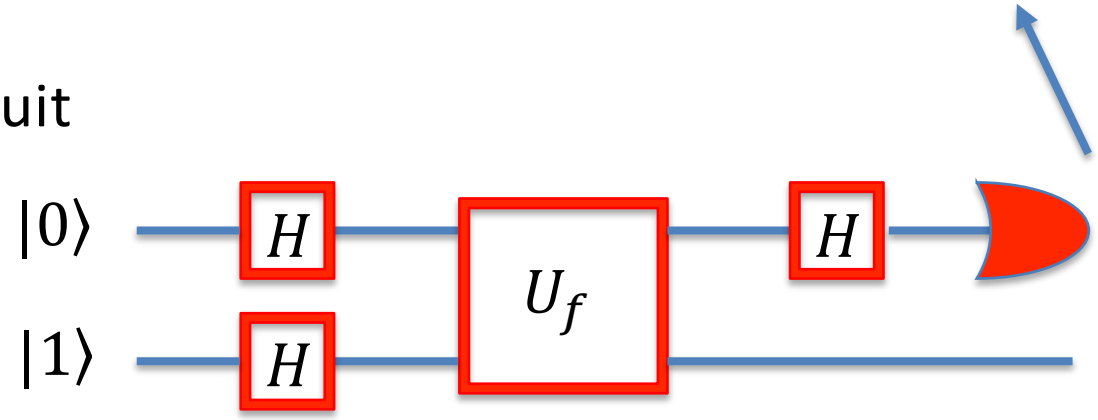
$$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \xrightarrow{H} \begin{matrix} ((-1)^{f(0)}+(-1)^{f(1)})|0\rangle \\ + \\ ((-1)^{f(0)}-(-1)^{f(1)})|1\rangle \end{matrix}$$

Step 4: getting the answer

If $f(0) = f(1)$ $\longrightarrow$ $|0\rangle$

If $f(0) \neq f(1)$ $\longrightarrow$ $|1\rangle$

Deustch circuit



Notice that the measurement does not determine which function is, only if It is constant or balance !!