QUANTUM COMPUTING

an introduction

Jean V. Bellissard

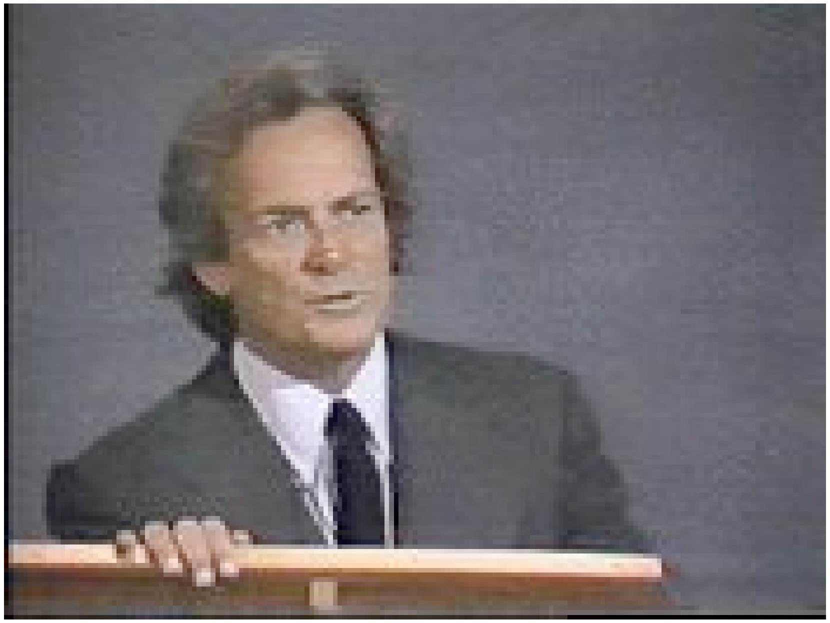
Georgia Institute of Technology
&
Institut Universitaire de France

A FAST GROWING SUBJECT:

elements for a history

Feynman's proposal:

He suggested in 1982 that quantum computers might have fundamentally more powerful computational abilities than conventional ones (basing his conjecture on the extreme difficulty encountered in computing the result of quantum mechanical processes on conventional computers, in marked contrast to the ease with which Nature computes the same results), a suggestion which has been followed up by fits and starts,and has recently led to the conclusion that either quantum mechanics is wrong in some respect, or else a quantum mechanical computer can make factoring integers "easy", destroying the entire existing edifice of publicKey cryptography, the current proposed basis for the electronic community of the future.



Richard P. Feynman.
Quantum mechanical computers.
Optics News,
11(2):11-20, 1985.

Deutsch's computer:

David Deutsch.
Quantum theory, the Church-Turing Principle and universal quantum computer.
***Proc. R. Soc. London A*,**
400, 11-20, (1985).

David Deutsch.
Conditional quantum dynamics and logic gates.
***Phys. Rev. Letters*,**
74, 4083-6, (1995).

Shor's algorithm:

This algorithm shows that a quantum computer can factorize integers into primes in polynomial time

Peter W. Shor.
Algorithm for quantum computation: discrete logarithms and factoring
Proc. 35th Annual Symposium on Foundation of Computer Science,
IEEE Press, Los Alamitos CA, (1994).

CSS error-correcting code:

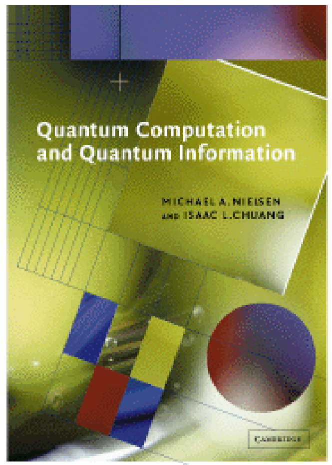

A. R. Calderbank &
B. P. W. Shor.
Good quantum error-correcting codes exist
***Phys. Rev. A,* 54, 1086, (1996).**

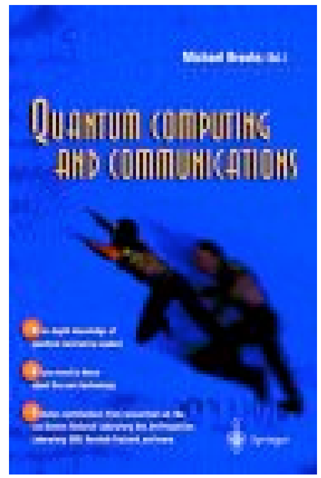
A. M. Steane
Error-correcting codes in quantum theory
***Phys. R. Letters,* 77, 793, (1996).**

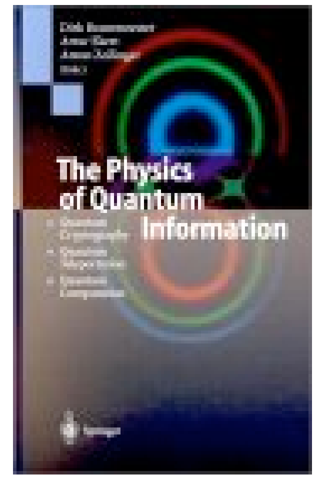
Topological error-correcting codes:

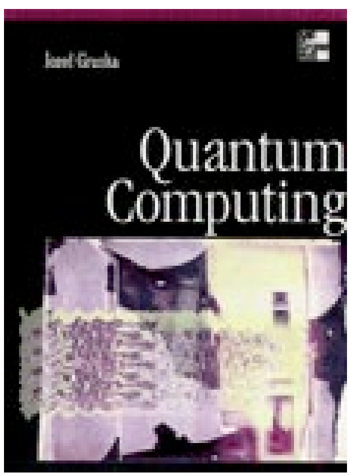
Alex Yu. Kitaev.
Fault-tolerant quantum computation by anyons
arXiv : quant-phys/9707021, (**1997**).

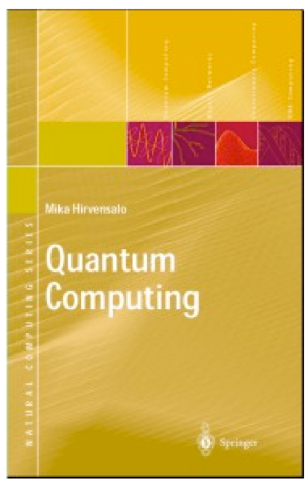
Books, books, books…

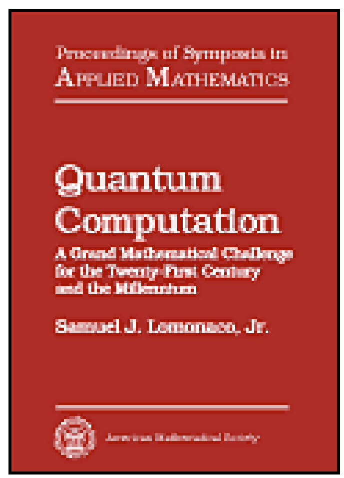


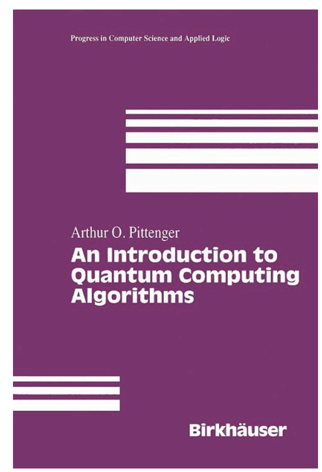












And much more at…

http://www.nsf.gov/pubs/2000/nsf00101/nsf00101.htm#preface
http://www.math.gatech.edu/~jeanbel/4803/

reports
articles,
books,
journals,

list of laboratories,
list of courses,
list of conferences,

QUBITS:

a unit of quantum information

10110101

Qubits:

- George BOOLE
  (1815-1864)
  used only two characters
  to code logical operations

0 1

Qubits:

- John von NEUMANN

  (1903-1957)

  developed the concept of programming using also binary system to code

  all information

0 1

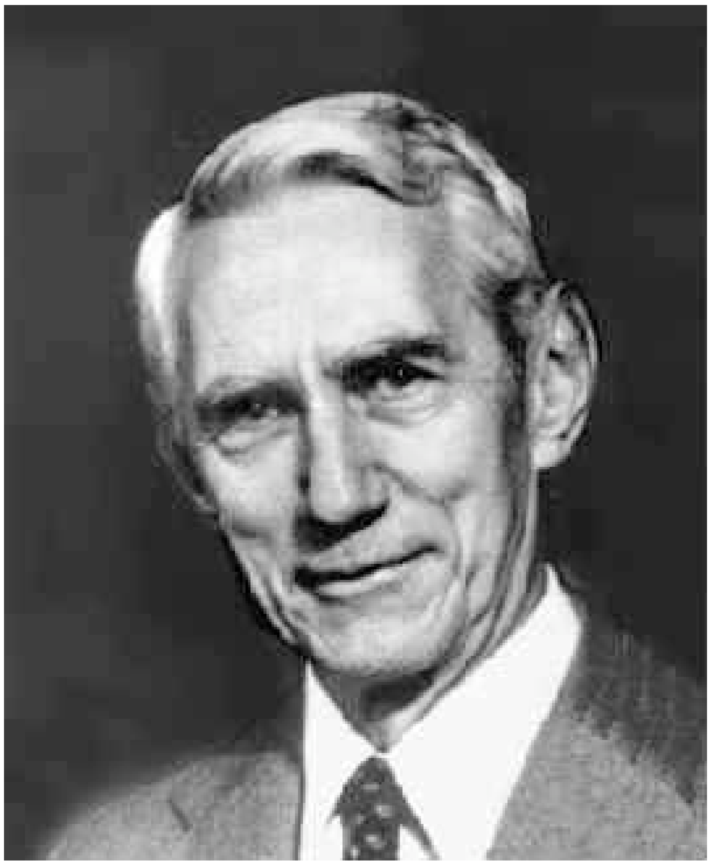
Qubits:

- Claude E. SHANNON

«A Mathematical Theory of Communication» (1948)

-Information theory

- unit of information ***bit***



0 1

Qubits:

1-qubit

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

quantizing $\longrightarrow$ *canonical basis in* $\mathbb{C}^2$

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

Qubits:

1 general qubit

$$|\,\square\,\rangle = \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix} = \mathbf{a}\,|0\rangle + \mathbf{b}\,|1\rangle$$

$$\langle\,\square\,| = (\mathbf{a}^*,\ \mathbf{b}^*) = \mathbf{a}^*\langle 0| + \mathbf{b}^*\langle 1|$$

*Dirac's **bra** and **ket** in $\mathbb{C}^2$ and its dual*

Qubits:

1 general qubit

$$| \, \square_i \rangle = \begin{pmatrix} \mathbf{a}_i \\ \\ \mathbf{b}_i \end{pmatrix} = \mathbf{a}_i \, |\mathbf{0}\rangle + \mathbf{b}_i \, |\mathbf{1}\rangle$$

$$\langle \, \square_1 \, | \, \square_2 \, \rangle = \mathbf{a}_1^{\,*} \mathbf{a}_2 + \mathbf{b}_1^{\,*} \mathbf{b}_2$$

inner product in $\mathbb{C}^2$ *using Dirac's notations*

Qubits:

1 general qubit

$$|\,\square_1 > < \square_2\,| = \begin{pmatrix} \mathbf{a}_1\,\mathbf{a}_2^{\,*} & \mathbf{a}_1\,\mathbf{b}_2^{\,*} \\ \mathbf{b}_1\,\mathbf{a}_2^{\,*} & \mathbf{b}_1\,\mathbf{b}_2^{\,*} \end{pmatrix}$$

$$\mathbf{Tr}\,(|\,\square_1 > < \square_2\,|) = < \square_2\,|\ \square_1 >$$

using Dirac's bra-ket's

Qubits:

1 general qubit

$$| \square \rangle = \begin{pmatrix} \mathbf{a} \\ \\ \mathbf{b} \end{pmatrix} = \mathbf{a}\, |\mathbf{0}\rangle + \mathbf{b}\, |\mathbf{1}\rangle$$

$$\langle \square \mid \square \rangle = |\mathbf{a}|^2 + |\mathbf{b}|^2 = \mathbf{1}$$

one qubit = element of the unit sphere in $\mathbb{C}^2$

Qubits:

1 general qubit

$$|\,\square\,\rangle = \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix} = \mathbf{a}\,|\mathbf{0}\rangle + \mathbf{b}\,|\mathbf{1}\rangle$$

$$|\,\mathbf{a}\,|^2 = \mathbf{Prob}\,(\mathbf{x=0}) = |\langle\square\,|\,\mathbf{0}\rangle|^2$$

$$|\,\mathbf{b}\,|^2 = \mathbf{Prob}\,(\mathbf{x=1}) = |\langle\square\,|\,\mathbf{1}\rangle|^2$$

Born's interpretation of a qubit

Qubits:

1 qubit: mixed states

$$|\Box\rangle\langle\Box| = \textbf{Projection on } \Box$$

$$p_i \geq 0 \, , \;\; \sum_i p_i = 1$$

$$\Box = \sum_i p_i \, |\Box_i\rangle\langle\Box_i|$$

$$\Box \geq 0 \, , \; \mathrm{Tr}(\Box) = 1$$

statistical mixtures of states:
density matrices

Qubits:

1 qubit: mixtures

Pauli matrices generate $M_2(C)$

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

Qubits:

1 qubit: mixtures

$$\rho \geq 0 \,,\ \mathrm{Tr}(\rho) = 1$$

$$\rho = (1 + a_x X + a_y Y + a_z Z)/2$$

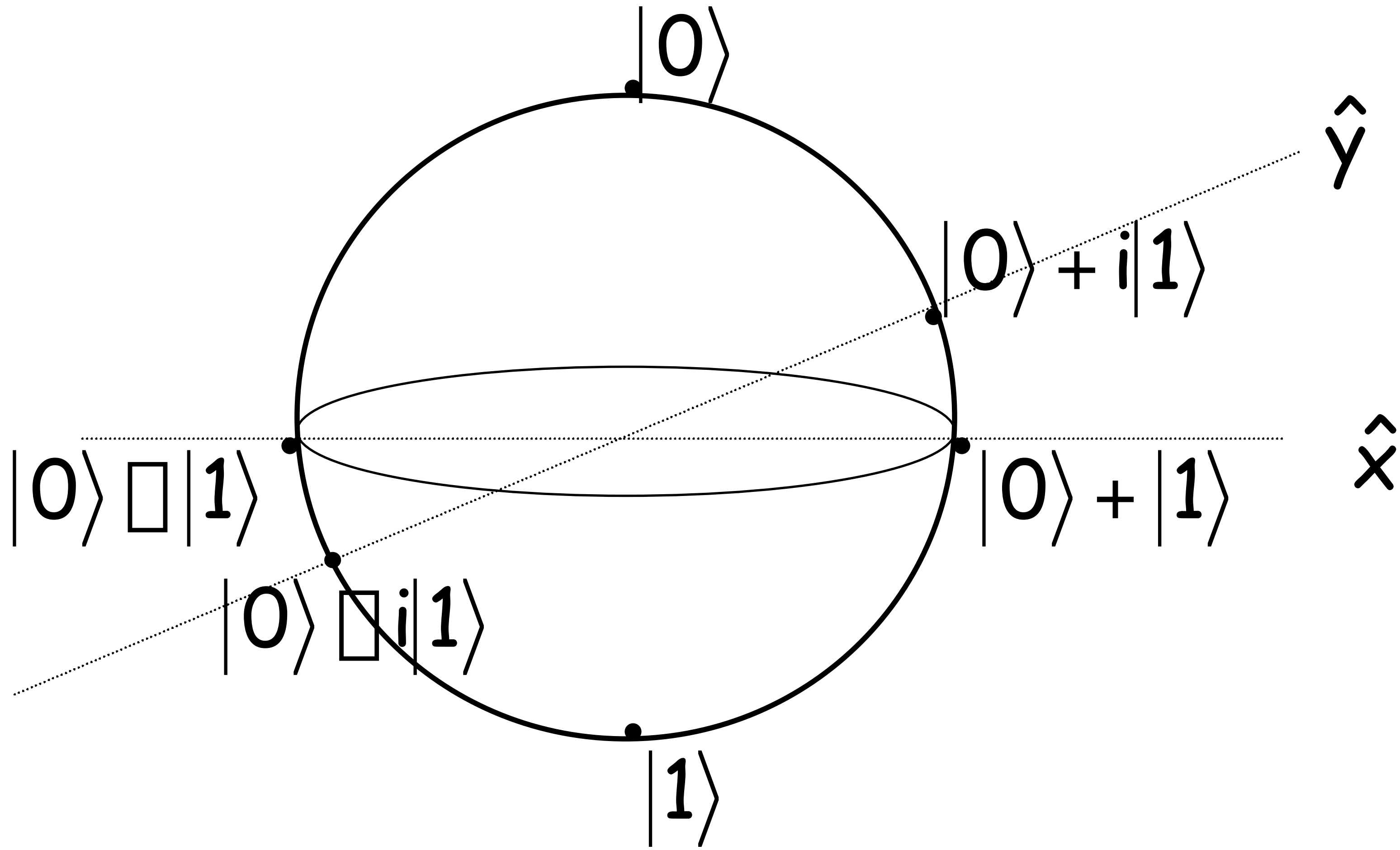
$$a_x^2 + a_y^2 + a_z^2 \leq 1$$

density matrices:

*the **Bloch** ball*

Qubits:

1 qubit: Bloch's ball



Qubits:

general N-qubits states

$$01001 \longrightarrow |\mathbf{01001}\rangle = |\mathbf{0}\rangle \otimes |\mathbf{1}\rangle \otimes |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle \otimes |\mathbf{1}\rangle$$

quantizing $\longrightarrow$ *tensor basis in* $\mathbb{C}^{2^n}$

Qubits:

general N-qubits states

$$|\psi\rangle = \sum \mathbf{a}(x_1,\ldots,x_N)\ |x_1\ldots x_N\rangle$$

$$\sum |\mathbf{a}(x_1,\ldots,x_N)|^2 = \mathbf{1}$$

entanglement*: an N-qubit state is* **NOT** *a* ***tensor product***

Qubits:

general N-qubits states

$$|\square_{00}\rangle = (|\mathbf{00}\rangle + |\mathbf{11}\rangle)/\sqrt{2}$$

$$|\square_{01}\rangle = (|\mathbf{01}\rangle + |\mathbf{10}\rangle)/\sqrt{2}$$

$$|\square_{10}\rangle = (|\mathbf{00}\rangle - |\mathbf{11}\rangle)/\sqrt{2}$$

$$|\square_{01}\rangle = (|\mathbf{01}\rangle - |\mathbf{10}\rangle)/\sqrt{2}$$

entanglement*: Bell's states*

QUANTUM GATES:

computing in quantum world

Quantum gates:

1-qubit gates

$$|x\rangle \;-\!\!-\!\!-\; \boxed{U} \;-\!\!-\!\!-\; U|x\rangle$$

U is unitary in $M_2(\mathbb{C})$

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

Pauli basis in $M_2(\mathbb{C})$

Quantum gates:

1-qubit gates

$$|x\rangle \;\text{———}\; \boxed{U} \;\text{———}\; U|x\rangle$$

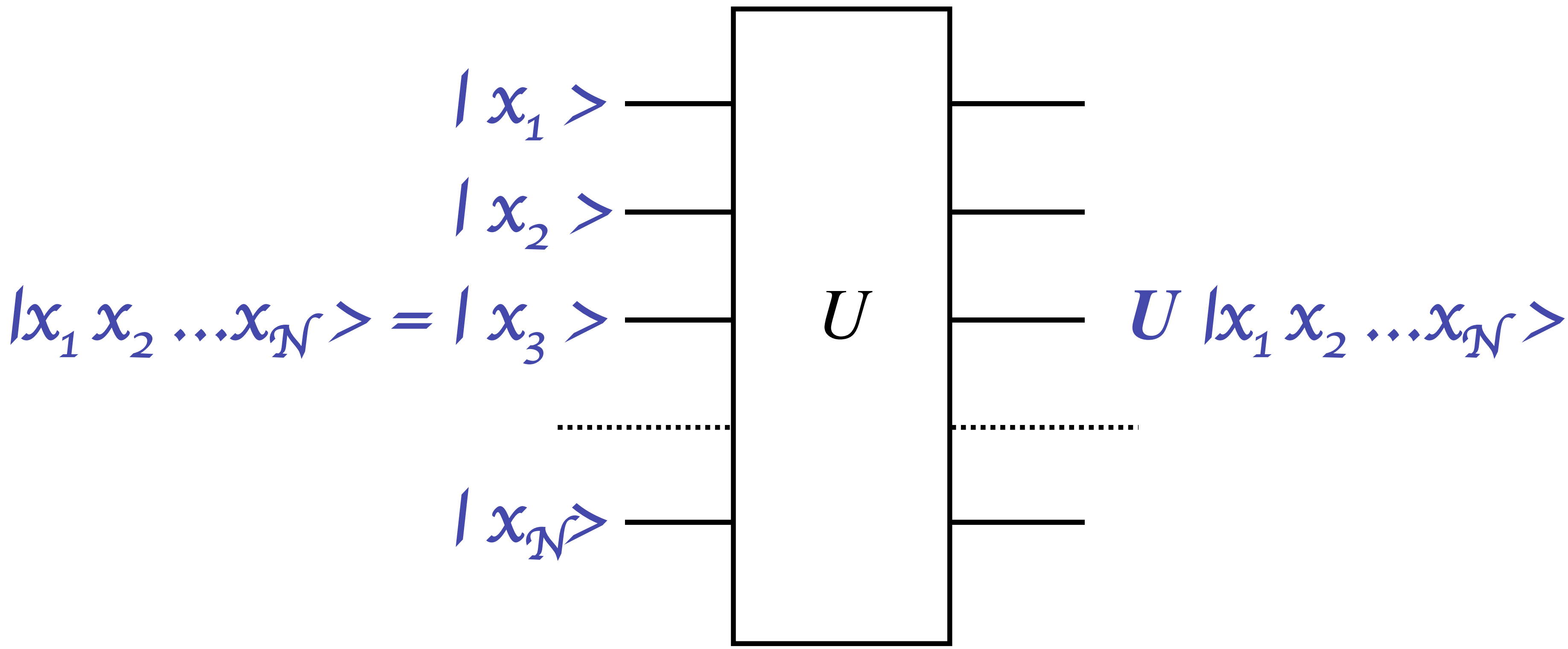
U is unitary in $M_2(\mathbb{C})$

$$H = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Hadamard, phase and $\pi/8$ *gates*

Quantum gates:

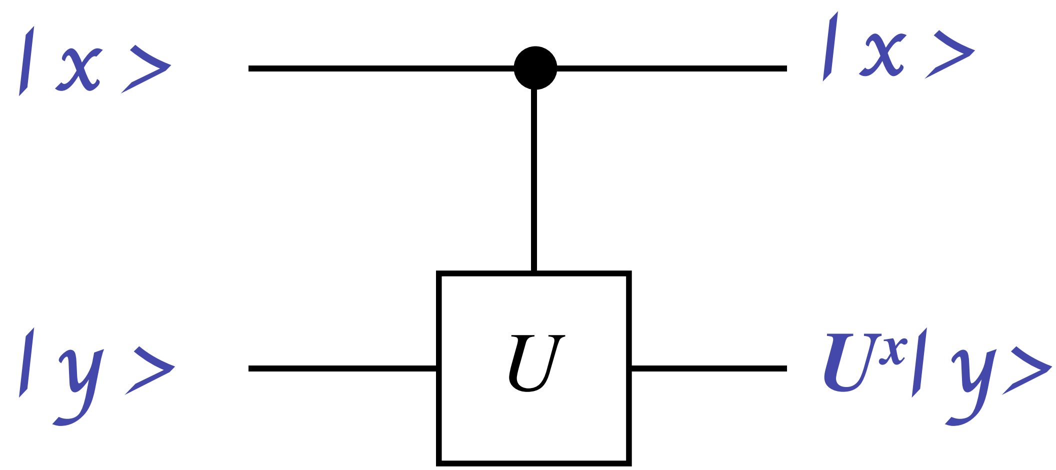
N-qubit gates



U is unitary in $M_{2^N}(\mathbb{C})$

Quantum gates:

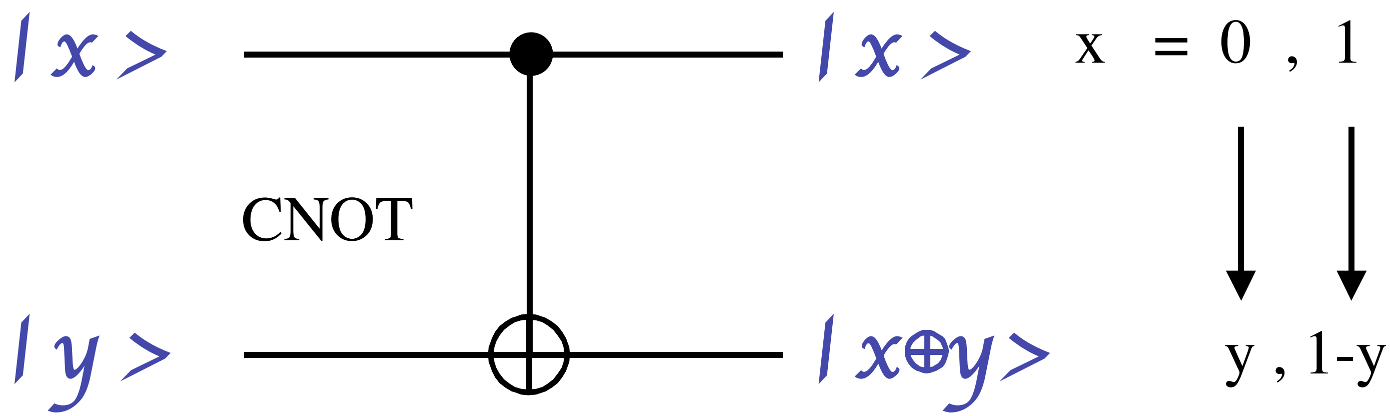
controlled gates



U is unitary in $M_2(\mathbb{C})$

Quantum gates:

controlled gates

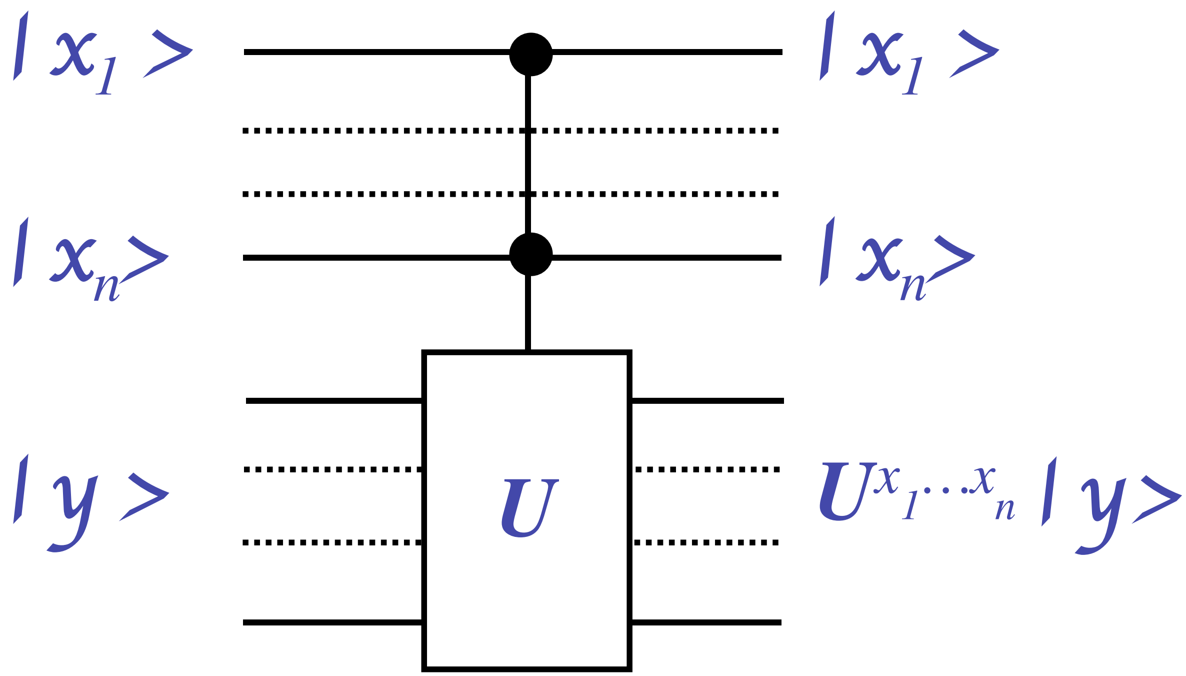


flipping a bit in a controlled way: the CNOT *gate*

$$U=X$$

Quantum gates:

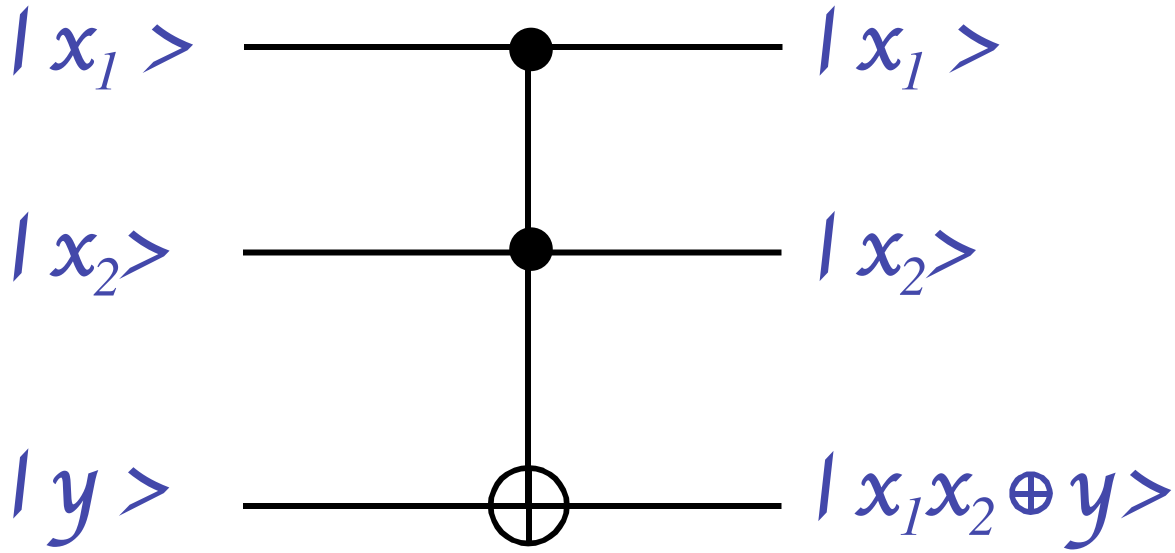
controlled gates



flipping bits in a controlled way

Quantum gates:

controlled gates



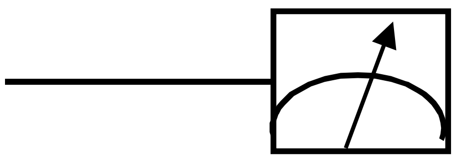
flipping bits in a controlled way

*The **Toffoli** gate*

QUANTUM CIRCUITS:

computing in quantum world

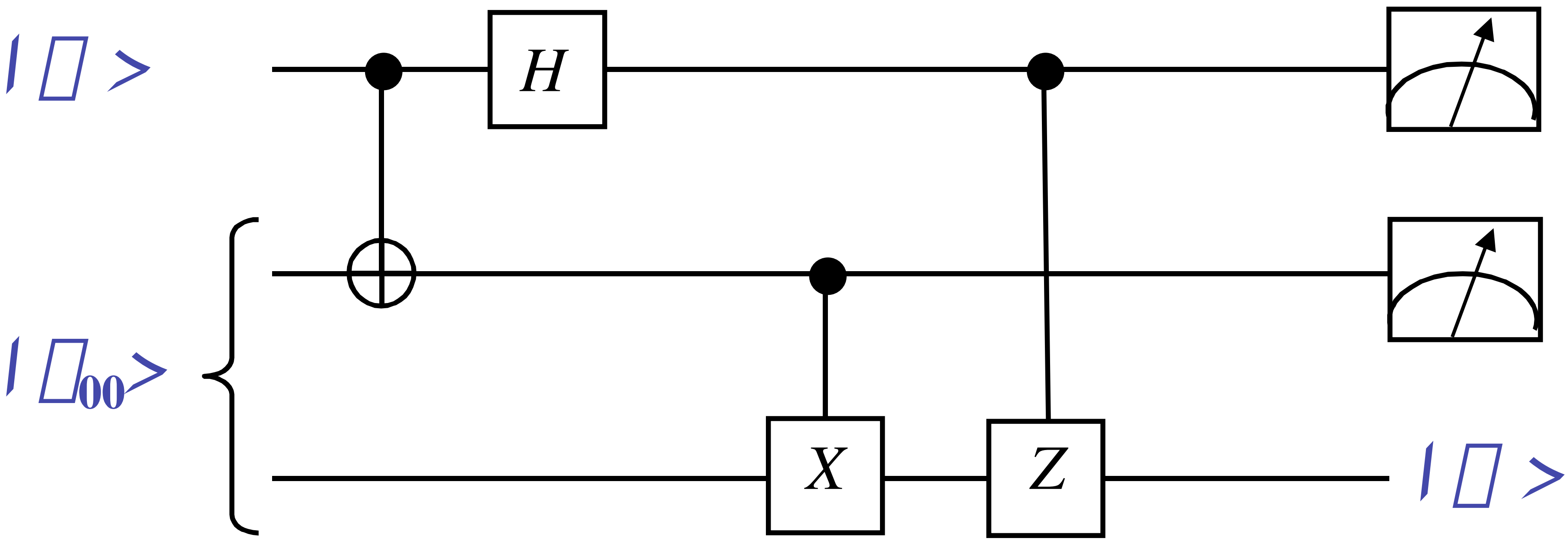
Quantum circuits: *measurement*



- Device that produces a value of the *bit* x
- The part of the state corresponding to this line is lost.

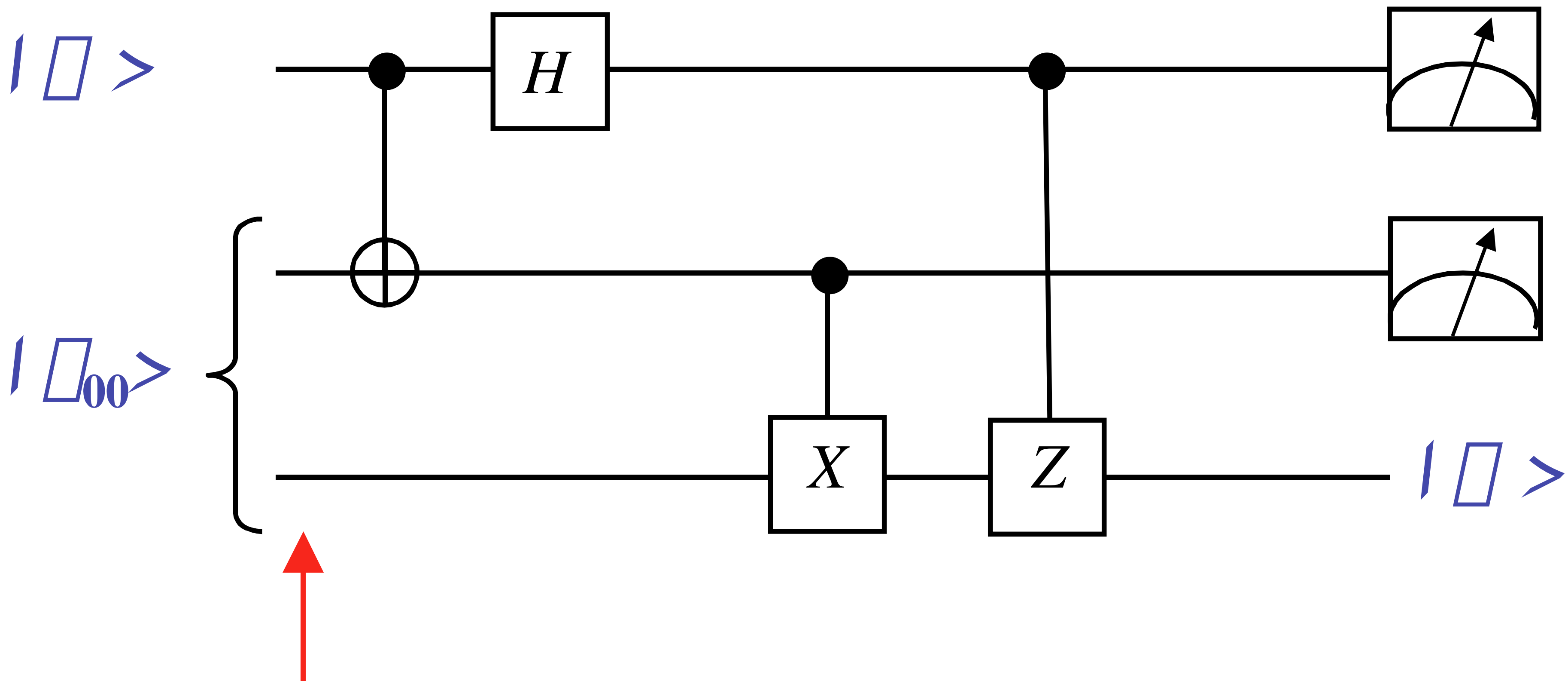
Quantum circuits:

teleportation



Quantum circuits:

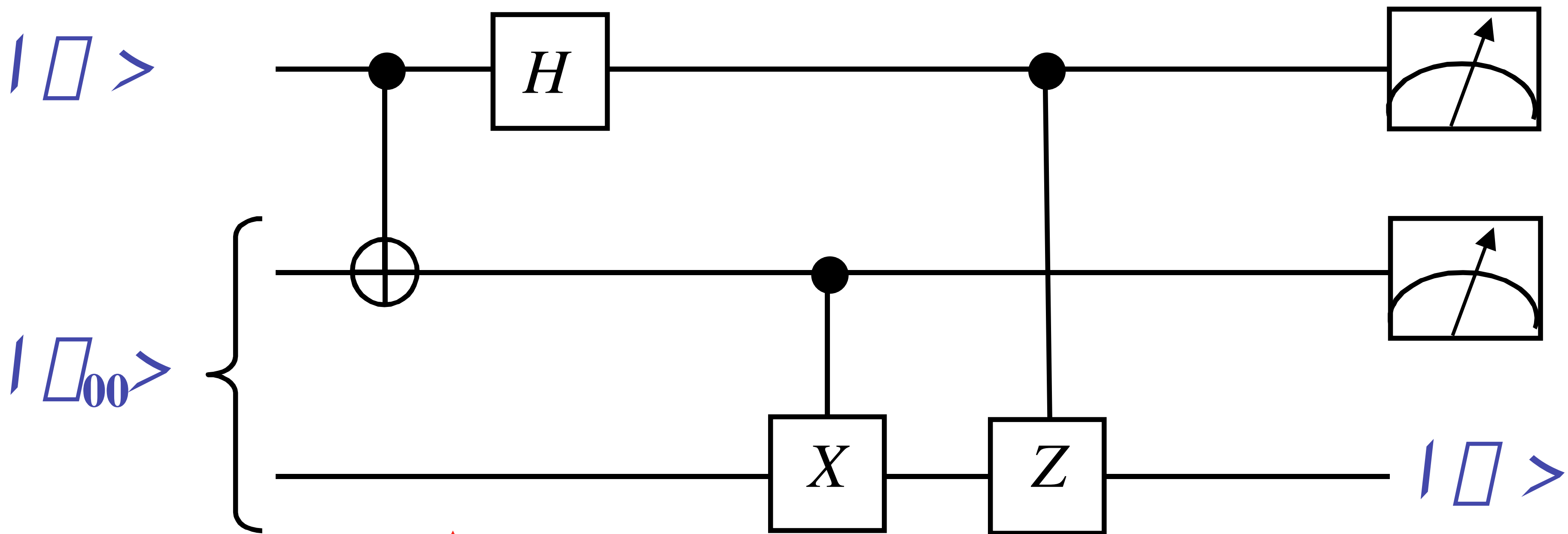
teleportation



$$\frac{|x00\rangle+|x11\rangle}{\sqrt{2}}$$

Quantum circuits:

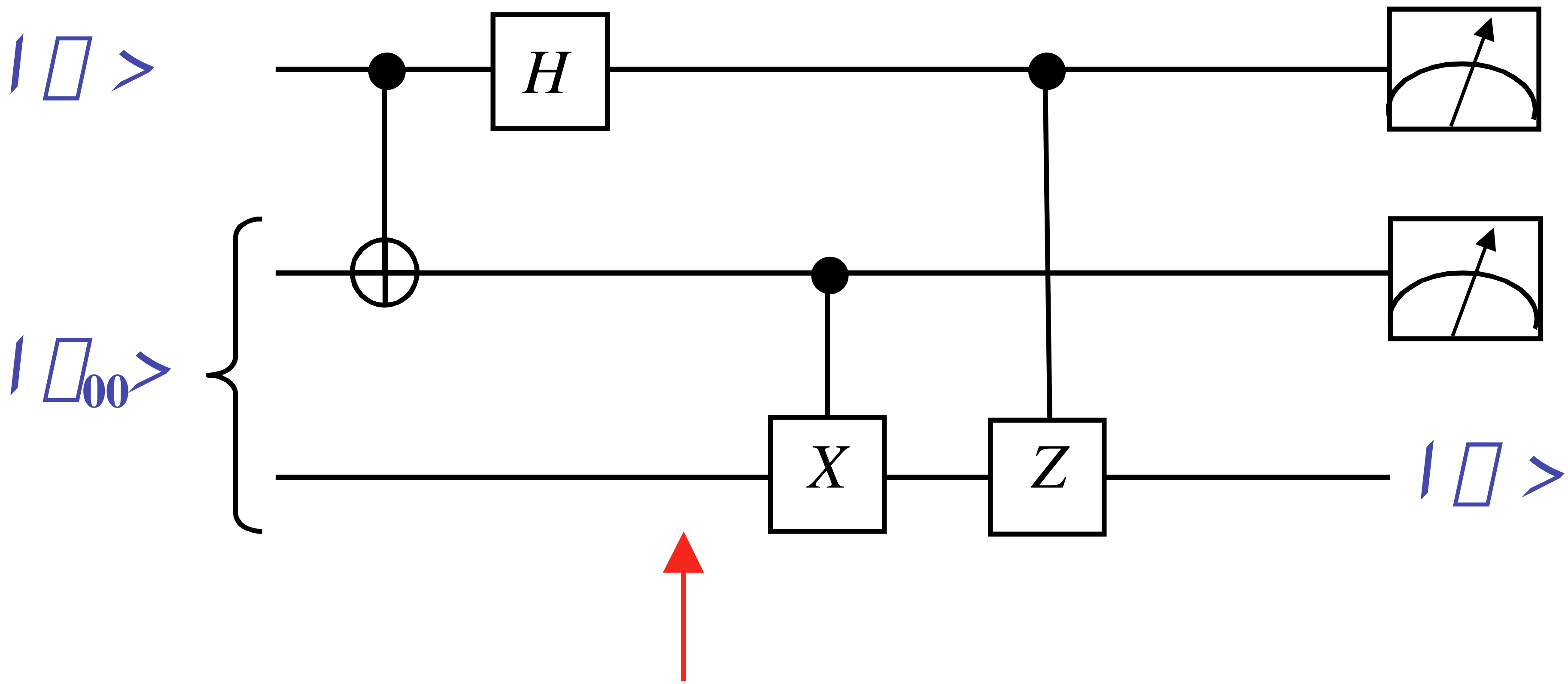
teleportation



$$\frac{|xx0\rangle + |x(1-x)1\rangle}{\sqrt{2}}$$

Quantum circuits:

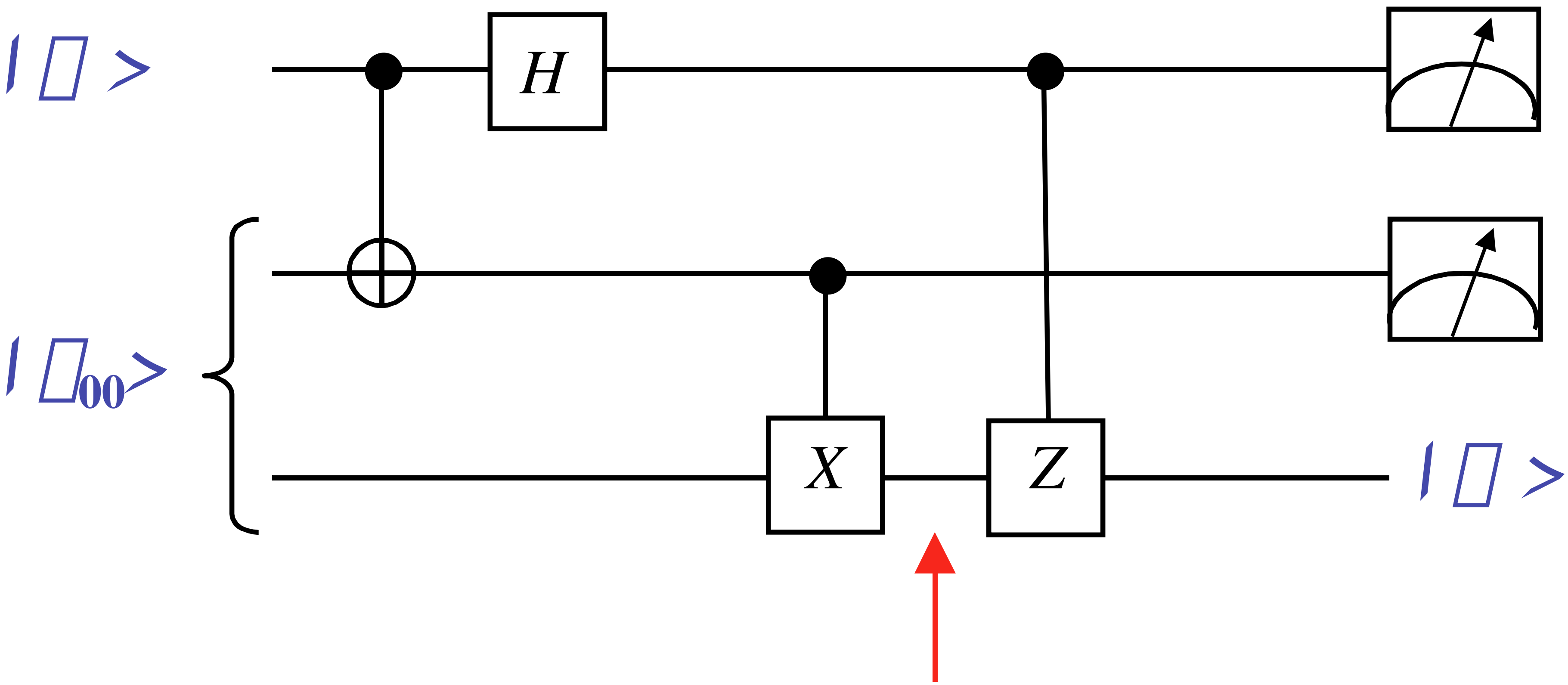
teleportation



$$\frac{(|0x0\rangle + (-)^{x}|1x0\rangle + |0\,(1\text{-}x)1\rangle + (-)^{x}|1\,(1\text{-}x)1\rangle)}{2}$$

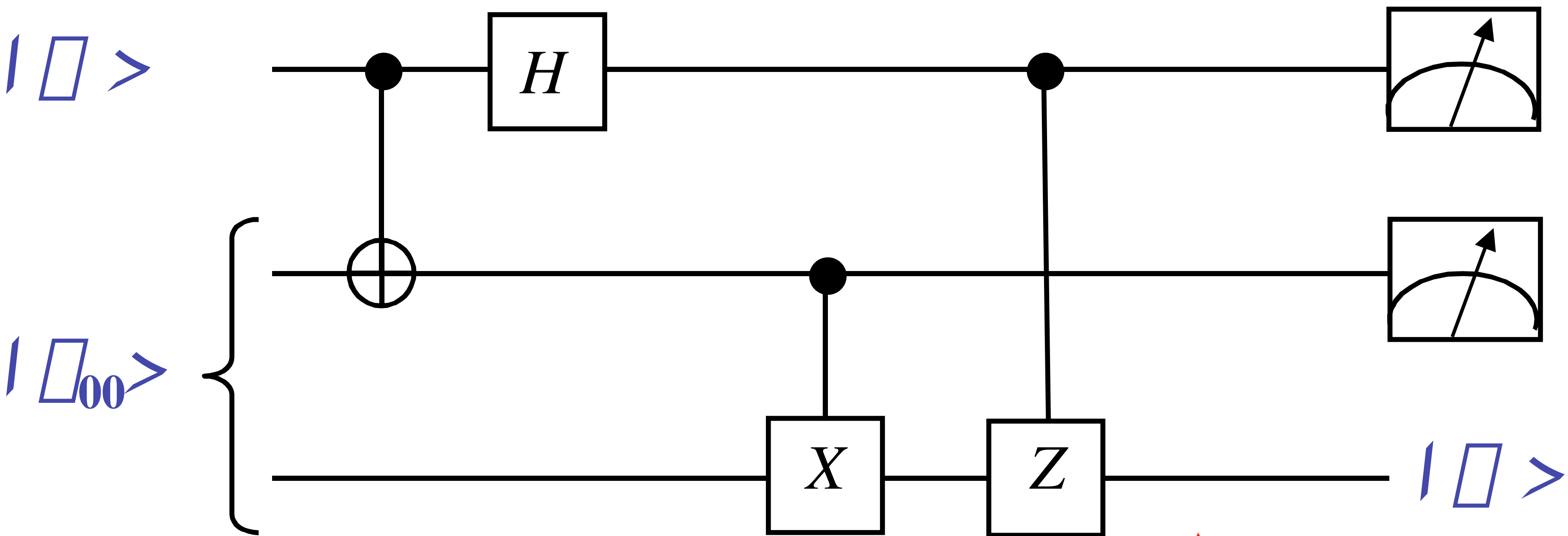
Quantum circuits:

teleportation



$$\frac{(|0xx\rangle+(-)^{x}|1xx\rangle+|0\,(1\text{-}x)\,x\rangle+(-)^{x}|1\,(1\text{-}x)x\rangle)}{2}$$

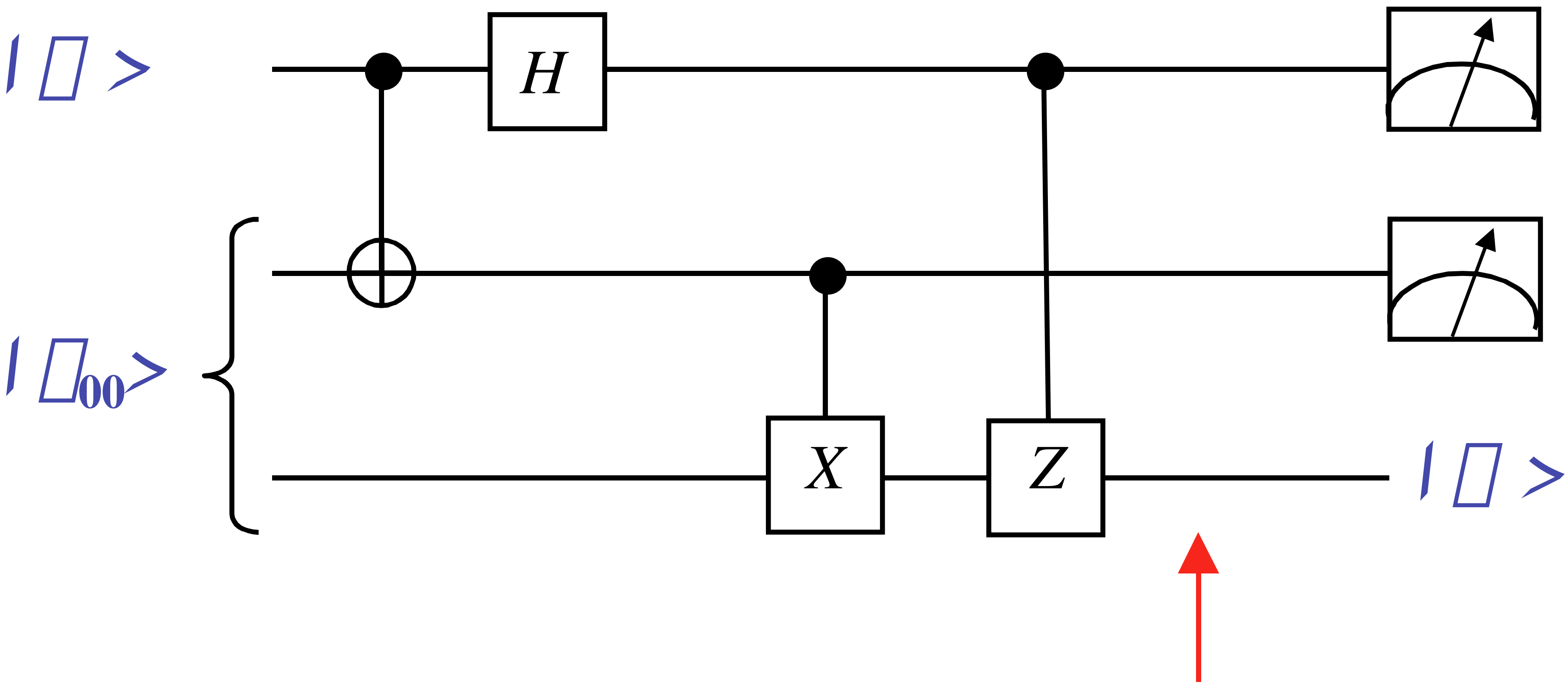
Quantum circuits: *teleportation*



$$\frac{\left(|0x\rangle + |1x\rangle + |0\,(1-x)\rangle + |1\,(1-x)\rangle\right)}{2} \otimes |x\rangle$$

Quantum circuits:

teleportation



$$\frac{(|00\rangle+|11\rangle+|01\rangle+|10\rangle)}{2} \otimes |x\rangle$$

QUANTUM COMPUTERS:

machines and laws of Physics

Computers:

Computers are machines obeying to laws of Physics:

- Non equilibrium Thermodynamics,
- Electromagnetism
- Quantum Mechanics

Computers:

Second Law of Thermodynamics

- Over time, the information contained in an isolated system can only be

  destroyed

- Equivalently, its entropy can only

  increase

Computers:

Computers are machines producing information:

- Coding, transmission, reconstruction
- Computation,
- Cryptography

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

0

coding

1

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

$0 \longrightarrow 000$

coding

$1 \longrightarrow 111$

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

$0 \xrightarrow{\text{coding}} 000$

$1 \rightarrow 111$

$\xrightarrow{\textit{Transmission}}$

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

$0 \rightarrow 000$ *Transmission* 010

coding $\longrightarrow$

errors

$1 \rightarrow 111$ *(2nd Law)* 110

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

0 → 000 | *Transmission* → *errors (2nd Law)* | 010 | *Reconstruction* →

coding

1 → 111 | | 110 |

Computers:

- *Coding theory uses redundancy to transmit binary bits of information*

$0 \rightarrow 000$	*Transmission*	010	*Reconstruction*	000
coding	$\longrightarrow$		$\longrightarrow$	
	errors		*at reception*	
$1 \rightarrow 111$	*(2nd Law)*	110	*(correction)*	111

Computers:

Principles of Quantum Mechanics

- States (*pure*) of a system are given by units vectors in a Hilbert space $\mathcal{H}$

- Observables are selfadjoint operators on $\mathcal{H}$ (Hamiltonian H, Angular momentum L, etc)

Computers:

Principles of Quantum Mechanics

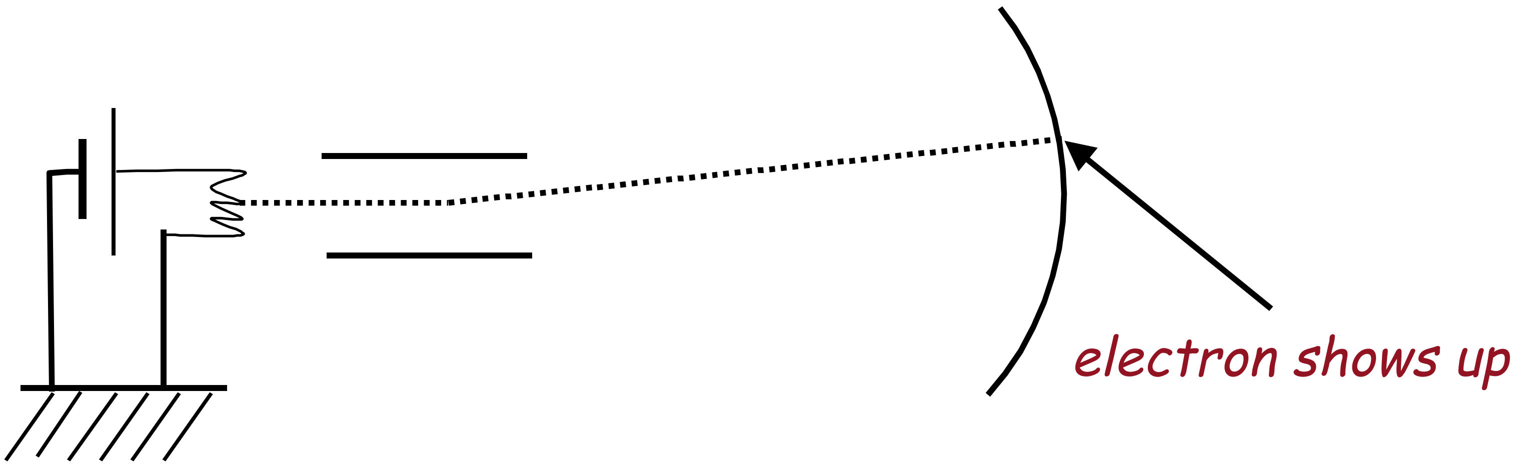
- Quantum Physics is fundamentally *probabilistic*:

  -theory can only predicts the probability distribution of a possible state or of the values of an observable

  -it cannot predict the actual value observed in experiment.

Computers:

Principles of Quantum Mechanics



Where one specific electron shows up is unpredictable
But the distribution of images of many electrons can be predicted

Computers:

Principles of Quantum Mechanics

- $|\langle \square | \square \rangle|^2$ represents the probability that $|\square\rangle$ is in the state $|\square\rangle$.

- Measurement of *A* in a state $\square$ is given by

$$\langle f(A)\rangle = \langle \square |\; f(A)\; | \square \rangle = \int d\mu_{\square}(a)\; f(a)$$

where $\mu_{\square}$ is the *probability distribution* for possible values of *A*

Computers:

Principles of Quantum Mechanics

- Time evolution is given by the Schrœdinger equation

  $$i\, d|\psi\rangle /dt = H\, |\psi\rangle \qquad\qquad H=H^*.$$

- Time evolution is given by the unitary operator e^{-itH} $\Rightarrow$ *no loss of information* !

Computers:

Principles of Quantum Mechanics

- Loss of information occurs:
  - in the *measurement* procedure
  - when the system interacts with the outside world (*dissipation*)
- Computing is much faster: the loss of information is postponed to the last operation

Computers:

Principles of Quantum Mechanics

- *Measurement* implies a loss of information (Heisenberg inequalities) requires *mixed* states
- Mixed states are described by *density matrices* with evolution

$$d\rho/dt = -i\,[H , \rho]$$

Computers:

Principles of Quantum Mechanics

- *Measurement* produces loss of information described by *a completely positive map* of the form

$$\mathcal{E}(\square) = \sum E_k \, \square \, E_k^*$$

  preserving the trace if

$$\sum E_k^* E_k = I \, .$$

- Each k represents one possible *outcome* of the measurement.

Computers:

Principles of Quantum Mechanics

- If the *outcome* of the measurement is given by k then the new state of the system *after* the measurement is given by

$$\rho_k = \frac{E_k \rho E_k^*}{Tr(E_k \rho E_k^*)}$$

Computers:

Principles of Quantum Mechanics

- In quantum computers, the result of a calculation is obtained through the measurement of the label indexing the digital basis
- The algorithm has to be such that the desired result is right whatever the outcome of the measurement !!

Computers:

Principles of Quantum Mechanics

- In quantum computers, *dissipative processes* (interaction within or with the outside) may destroy partly the information unwillingly.
- *Error-correcting* codes and *speed* of calculation should be used to make dissipation harmless.

TO CONCLUDE (PART I):

quantum computers may work

To conclude (part I)

- The elementary unit of quantum information is the *qubit*, with states represented by the *Bloch ball*.
- Several qubits are given by tensor products leading to *entanglement*.
- Quantum gates are given by unitary operators and lead to quantum circuits
- Law of physics must be considered for a quantum computer to work: measurement, dissipation…

See you next week !!