Summer School on Modern Quantum Technologies, BITP, Kiev
September 12th 2018

Quantum computation from the physicist's viewpoint

Sergey N. Shevchenko

B. Verkin Institute for Low Temperature Physics and Engineering, Kharkov

Quantum vs. “classical” computer

LOCKHEED MARTIN

Google

Los Alamos NATIONAL LABORATORY EST. 1943

NASA

The computer D-Wave 2000Q™: has 2048 superconducting qubits [my second lecture] from Niobium at 15 mK.

{cf. Experimental Ten-Photon Entanglement, PRL 117, 210502 (2016)}

Agenda

Qubits

Single-qubit operations

Controlled-not operation

Quantum schemes

Quantum teleportation and parallelism – the homework

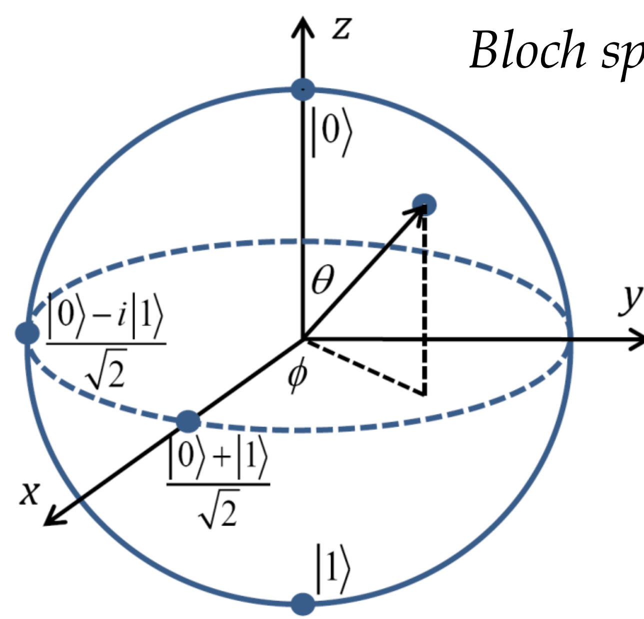
A BIT ABOUT QUBITS

A qubit, is in principle any quantum system with two possible states. General theory of quantum computation and information is built on the notion of an abstract qubit, not detailing its physical origin.

Qubit vector-state: $$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

Basis states: $$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Bloch sphere



For graphic illustration:

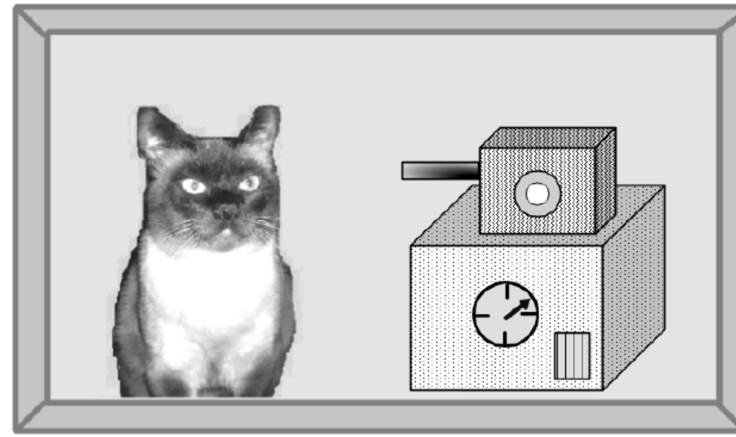
$$\alpha = \cos\frac{\theta}{2},$$
$$\beta = e^{i\varphi}\sin\frac{\theta}{2}$$

SUPERPOSITION and ENTANGLEMENT – resources for quantum technologies

Remark 1 – Schrodinger-cat paradox:
let the cat state $|\downarrow / \uparrow\rangle$
depend on the radioactive atom state $|0/1\rangle$.

Then the system can be considered as being in an entangled state:

$$\left|\Psi\right\rangle = \alpha\left|0,\uparrow\right\rangle + \beta\left|1,\downarrow\right\rangle.$$



Remark 2 **–** about the superposition state $\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$

This can be interpreted as a qubit in states 0 and 1 simultaneously.

Two qubits can simultaneously take four values – 00, 01, 10 and 11.

Each additional qubit doubles the number of possible states.

For n qubits there are 2^n possible states.

And a quantum register of only 350 qubits can support 2^{350} values simultaneously. This is more than the number of atoms in the visible part of the universe, and more than the *googol* = 10^{100}.

Remark about the two-qubit states

General state:

$$|\Psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle, \qquad |ij\rangle = |i\rangle \otimes |j\rangle$$

Separable state - example:

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

Entangled state - example:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

=> Einstein-Podolsky-Rosen paradox (effect!)

EXAMPLE OF A QUBIT: SPIN-1/2

The Hamiltonian of a particle with a spin in the electromagnetic field has the form

$$H = \frac{1}{2m}\left(\vec{p} - \frac{e}{c}\vec{A}\right)^2 + e\varphi - \vec{\mu}\vec{H}.$$

For a particle with spin $s = 1/2$, the spin operator is given by the Pauli matrices, and the Hamiltonian equals

$$H = \frac{1}{2}\mathrm{g}\mu_{\mathrm{B}}\vec{\sigma}\vec{H},$$

$$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z), \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In general case, it is interesting to formulate the problem, when there are constant and alternating components of the magnetic field. Choosing the former along the x axis and the latter along the z axis and introducing evident change in notations, we obtain

$$H = -\frac{\Delta}{2}\sigma_x - \frac{\varepsilon(t)}{2}\sigma_z.$$

With this Hamiltonian, we can describe dynamical phenomena, like Rabi oscillations…

SINGLE-QUBIT OPERATIONS: Unitarity

The coefficients in $\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ satisfy $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1.$

This condition has also to be satisfied by $\left|\psi'\right\rangle = U\left|\psi\right\rangle = \alpha'\left|0\right\rangle + \beta'\left|1\right\rangle.$

Then it follows: $\left\langle\psi'\middle|\psi'\right\rangle = \left\langle\psi\middle|U^\dagger U\middle|\psi\right\rangle = 1 \;\Rightarrow U^\dagger U = I.$

The unitarity is the only restriction for the quantum operations.
In other words, any unitary matrix defines some quantum operation.
This is in contrast with the classical case, where there is only one nontrivial single-bit operation, NOT.

Consider next the most important quantum single-qubit operations.

SINGLE-QUBIT OPERATIONS

First, the operations defined by the Pauli matrices:

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Their action is described as follows:

$$X\left|0\right\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left|1\right\rangle.$$

Other useful operations – Hadamard (H), phase shift (S), and $\pi/8$ - element (T):

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

The Hadamard gate creates superposition states:

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}. \qquad \text{Or:} \quad \left|0\right\rangle \xrightarrow{H} \left(\left|0\right\rangle + \left|1\right\rangle\right)/\sqrt{2}.$$

SINGLE-QUBIT OPERATIONS
graphic presentation

Logic NOT, Z, and Hadamard operations:

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{X}—\; \beta|0\rangle+\alpha|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle-\beta|1\rangle$$

$$\alpha|0\rangle+\beta|1\rangle \;—\boxed{H}—\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

And this is a useful task to check these.

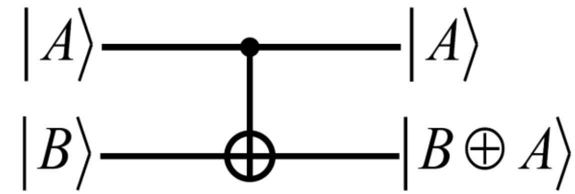
Controlled-NOT (CNOT) operation: definition

This is defined by the impact of the first (control) qubit onto the second (target) qubit, so that the value of the latter is changed only if the value of the former is 1. Namely:

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

Equivalently: $|A,B\rangle \rightarrow |A, B \oplus A\rangle$,

Respective "algorithm":



Controlled-NOT (CNOT) operation: matrix

This is defined by the impact of the first (control) qubit onto the second (target) qubit, so that the value of the latter is changed only if the value of the former is 1. Namely:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle.$$

For the matrix representation, remind, first, the tensor product:

$$|\psi_1, \psi_2\rangle \equiv |\psi_1\rangle |\psi_2\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \beta \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix} \equiv \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}.$$

This means that the basis vectors have the form:

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

Then we have:

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

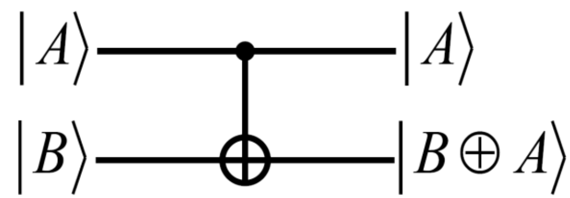
Controlled-NOT (CNOT) operation & the statement

This is defined by the impact of the first (control) qubit onto the second (target) qubit, so that the value of the latter is changed only if the value of the former is 1. Namely:

$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle.$$

Equivalently: $|A, B\rangle \to |A, B \oplus A\rangle,$

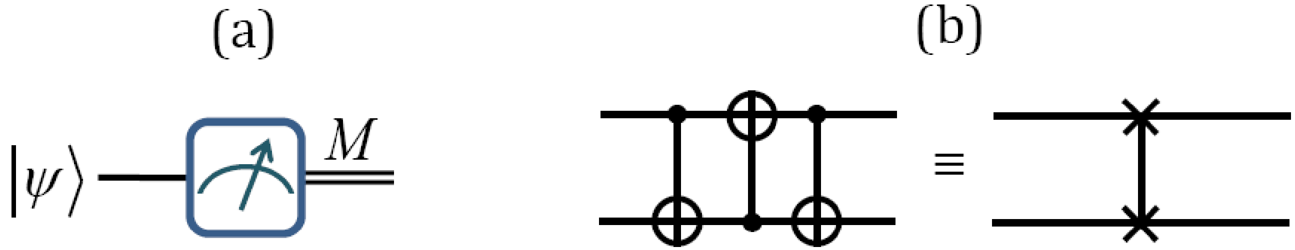
Respective "algorithm":



The statement: (see §4.5 in [Nielsen and Chuang 2010]) arbitrary operation on the space of states of n qubits can be realized using only one-qubit elements together with the CNOT element.

Thus, we know everything needed to write quantum algorithms!

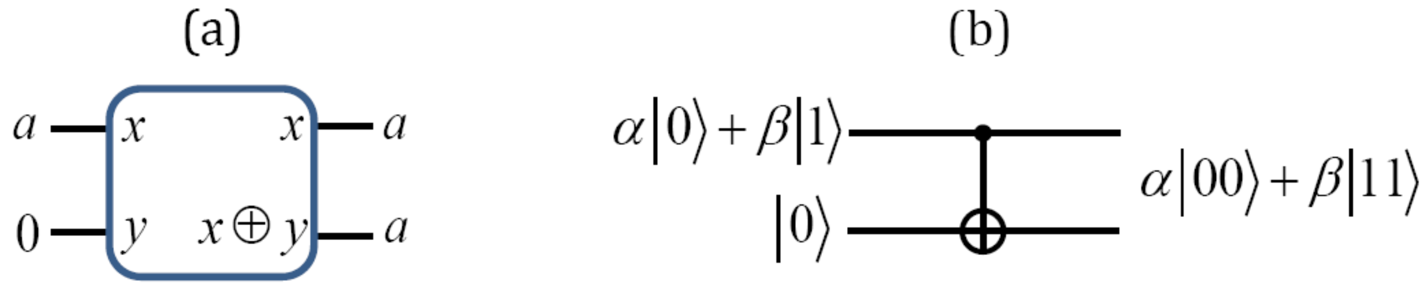
Several QUANTUM SCHEMES:
1. Measurement and swap operation



(a) The measurement operation gives a classical bit *M*.
For the state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ this bit is 0 with the probability $|\alpha|^2$ and 1 with the probability $|\beta|^2$.

(b) Swap operation: $|a,b\rangle \rightarrow |b,a\rangle$.
One can check this as follows: $|a,b\rangle \rightarrow |a, a\oplus b\rangle \rightarrow \ldots \rightarrow |b,a\rangle$.

Several QUANTUM SCHEMES:
2. No-cloning theorem



(a) Classical copying of a bit can be realized by means of the controlled-NOT operations.

(b) Let us now try to copy analogously the state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
Then we get:

$$\left[\alpha|0\rangle + \beta|1\rangle\right]|0\rangle = \alpha|00\rangle + \beta|10\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle.$$

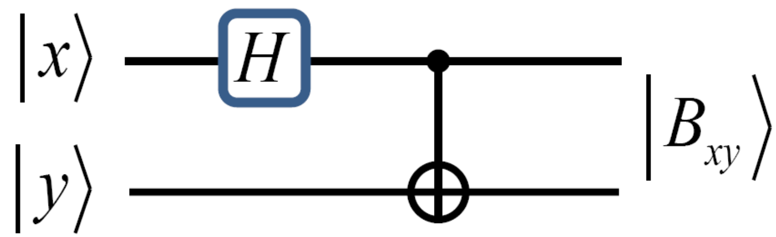
However, in general case, we would expect

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle.$$

So, **<u>it is impossible to copy an arbitrary quantum state.</u>** (More precisely, the cloning operation can copy only orthogonal states, here – |0> and |1>.)

Several QUANTUM SCHEMES:
3. Creation of the Bell states

These can be introduced as the states derived from the basis states, by making use of the Hadamard operation and the controlled-NOT operation



Indeed we obtain:

$$|00\rangle = |0\rangle|0\rangle \xrightarrow{H_1} \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{CNOT} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

This creates the Bell states from the basic states:

$$|00\rangle \to \frac{|00\rangle + |11\rangle}{\sqrt{2}} \equiv |B_{00}\rangle, \quad |01\rangle \to \frac{|01\rangle + |10\rangle}{\sqrt{2}} \equiv |B_{01}\rangle,$$

$$|10\rangle \to \frac{|00\rangle - |11\rangle}{\sqrt{2}} \equiv |B_{10}\rangle, \quad |11\rangle \to \frac{|01\rangle - |10\rangle}{\sqrt{2}} \equiv |B_{11}\rangle.$$

HOMEWORK: Quantum parallelism

Quantum parallelism is a principal feature distinguishing quantum computers from classical ones. This assumes the ability of simultaneous calculation of a binary function f(x) for diverse values x. Consider, for illustration, a problem of "how to see two sides of a coin simultaneously".

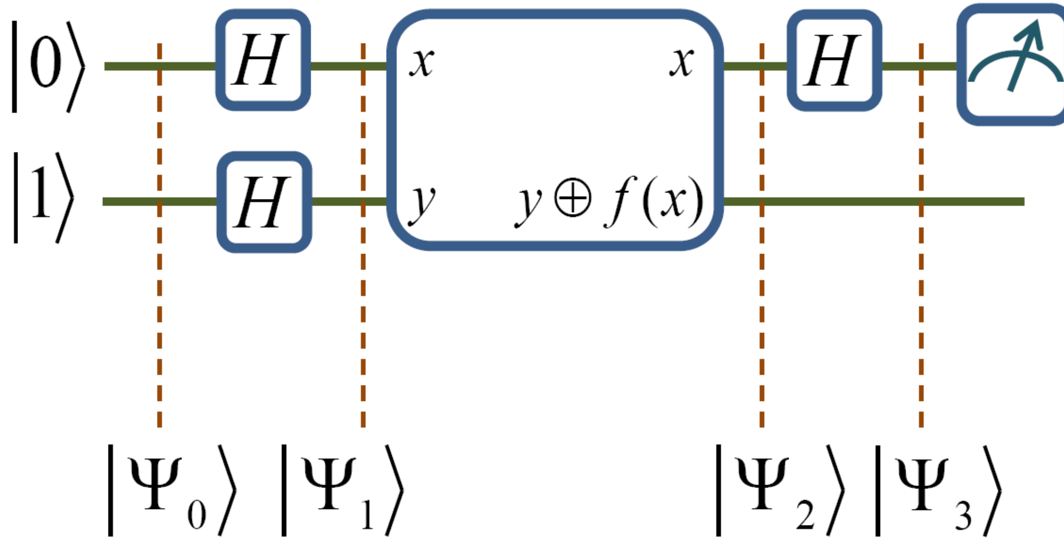
a = (0,1) (coin side)

$f(a)$ = (0,1) (heads/tails)

$f(a)$ = const or not?

[$f(a)$ = 0, 1, a, not(a)]

How many measurements?!



$|\Psi_0\rangle = |01\rangle \equiv |0\rangle|1\rangle$ - initial state

$|\Psi_1\rangle = \ldots$ - superposition state

...

$$|\Psi_3\rangle = |f(0) \oplus f(1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

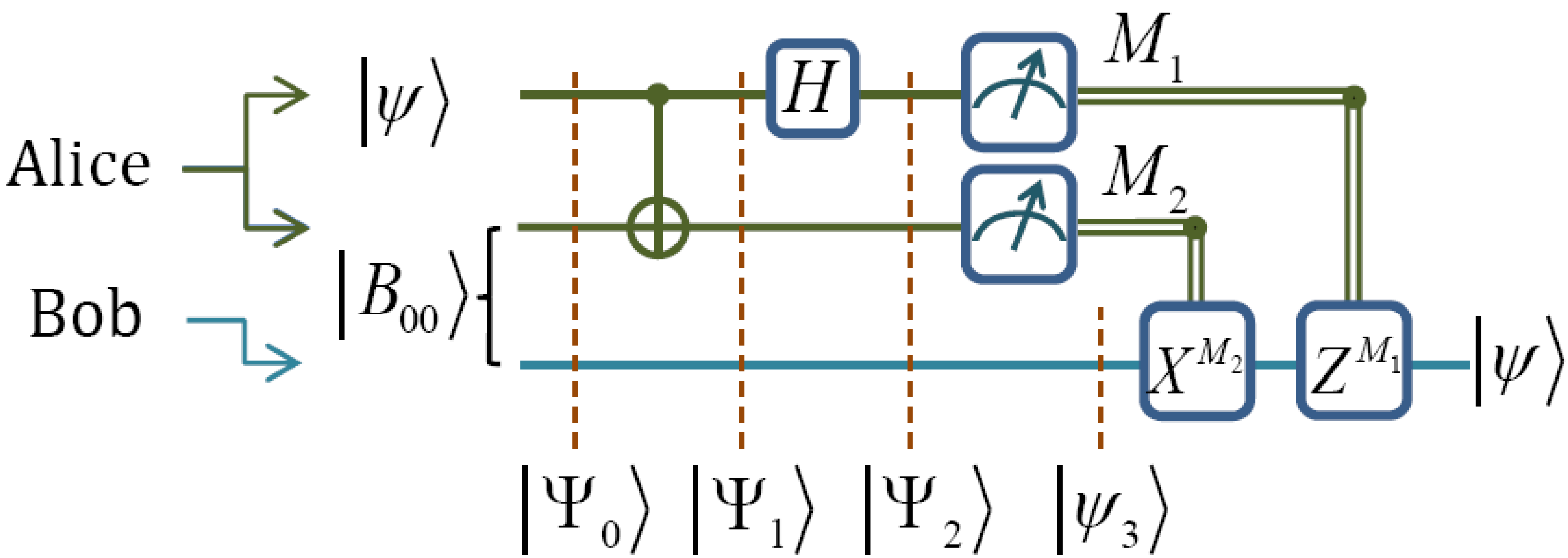
$f(0) \oplus f(1) = 0 \Rightarrow f(a) = const$ - false

$f(0) \oplus f(1) = 1 \Rightarrow f(a) \neq const$ - not false

HOMEWORK: Quantum teleportation

which is the technique of transferring quantum information without physically sending qubits.

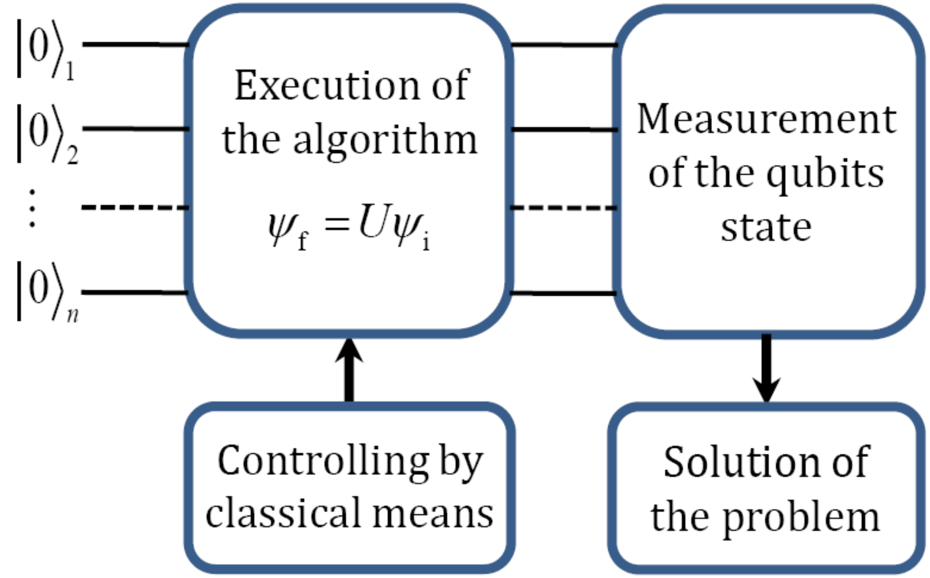
Consider transferring quantum information from Alice to Bob. Assume they have one part of an EPR pair each. Alice via classical channel tells the result of a measurement provided on her side to Bob, and he immediately obtains the state of the Alice's qubit before measurement.



The task is to describe this, by writing down the wave functions after each operation and to convince that the state of the Bob's qubit will be the same, as Alice had.

CONCLUSIONS

- Quantum technologies are based on the laws of quantum mechanics
- Quantum computer is described by unitary operations on qubits
- Single-qubit operations and CNOT allow us to describe: projective measurement, no-cloning theorem, Bell states, quantum parallelism (Deutch algorithm), quantum teleportation…



FOR FURTHER READING

M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (CUP, Cambridge, 2010); (Mir, Moscow, 2006).

K. A. Valiev, Quantum computers and quantum computations, Physics-Uspekhi **48**, 1 (2005); UFN **175**, 3 (2005),

…

REQUIREMENTS for the candidates in qubits (DiVincinzo criteria)

(1) **Scalability**. We need to have a scalable system of qubits with well-defined parameters and with the ability to create the entangled states. In particular, this means that the upper levels of the physical realization of the qubit device are well separated from the operational two levels.

(2) **Initialization**. There should be the ability to prepare given states. For computations this initial state can be the ground state. Then in practice this can be reached by the cooling.

(3) **Isolation**. Good isolation from the environment and large decoherence times are needed. These times should be at least three orders of magnitude larger than a characteristic time needed for an operation, so that to have the ability to work with the information before it is lost, to transmit the information and to initialize the quantum error correction algorithms.

(4) **Control**. We should have the ability to make one- and two-qubit unitary operations. It was proven that these are sufficient for all the problems on multi-qubit systems.

(5) **Measurement**. For finalizing quantum algorithms, we need the capability to reliably measure the states of individual qubits.

Candidates for qubits

Microscopic:

ions in electromagnetic traps,

polarized states of photons in resonator,

nuclear spins of molecules,

…

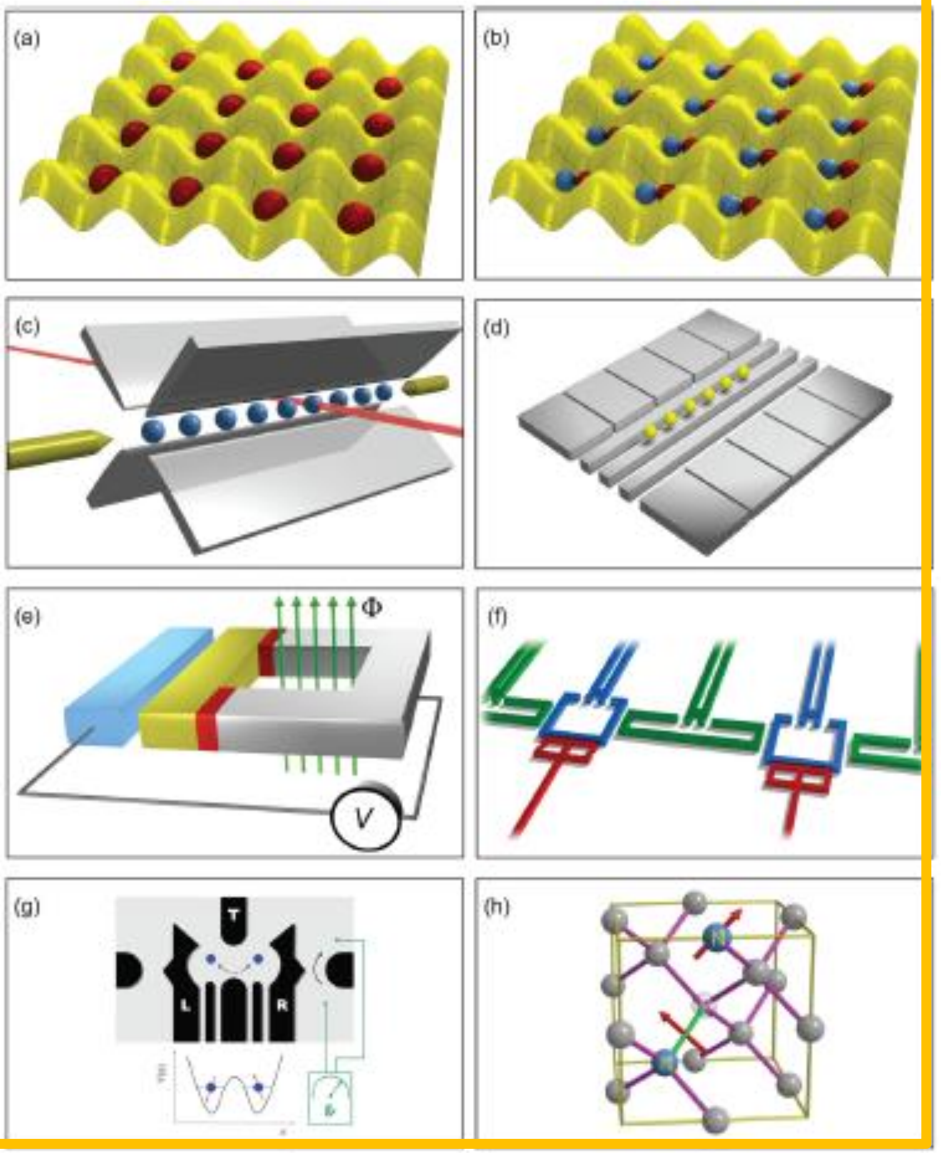
Mesoscopic:

electron states in quantum dots,

magnetic nanoparticles,

charge and phase in Josephson structures,

…



[Buluta, Ashhab, Nori, Rep. Prog. Phys. (2011)]