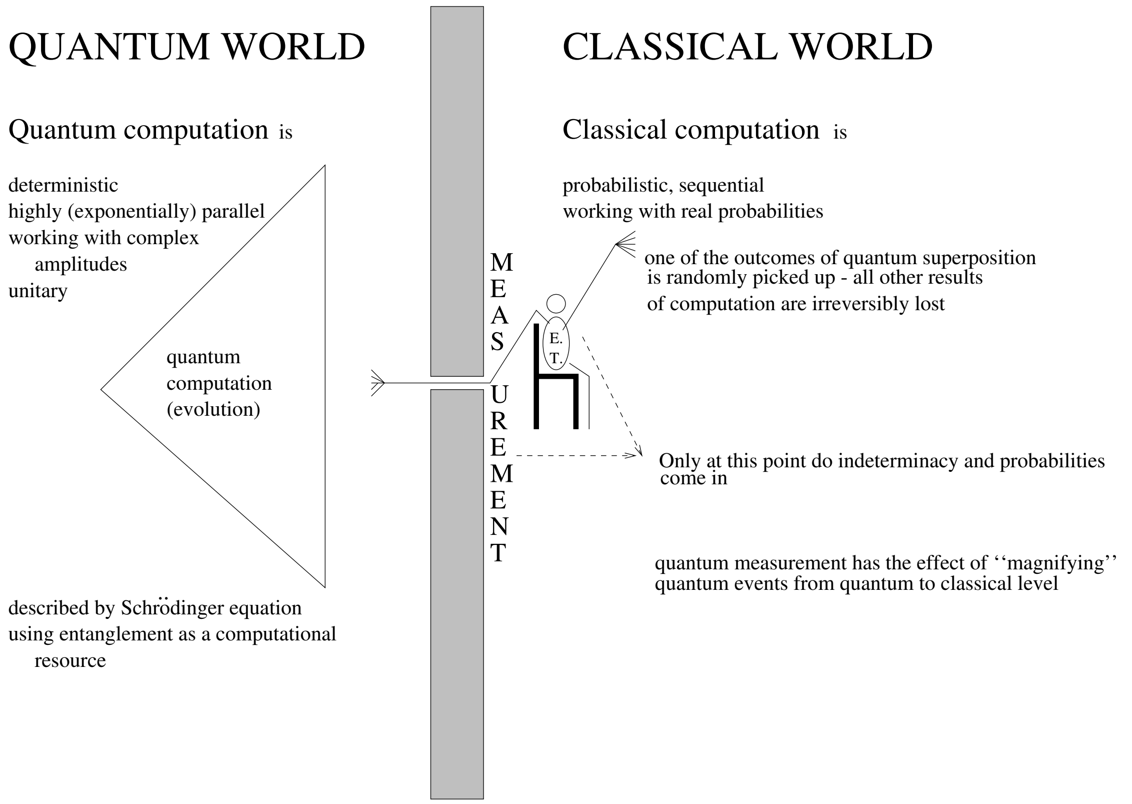


QUANTUM COMPUTING 1.

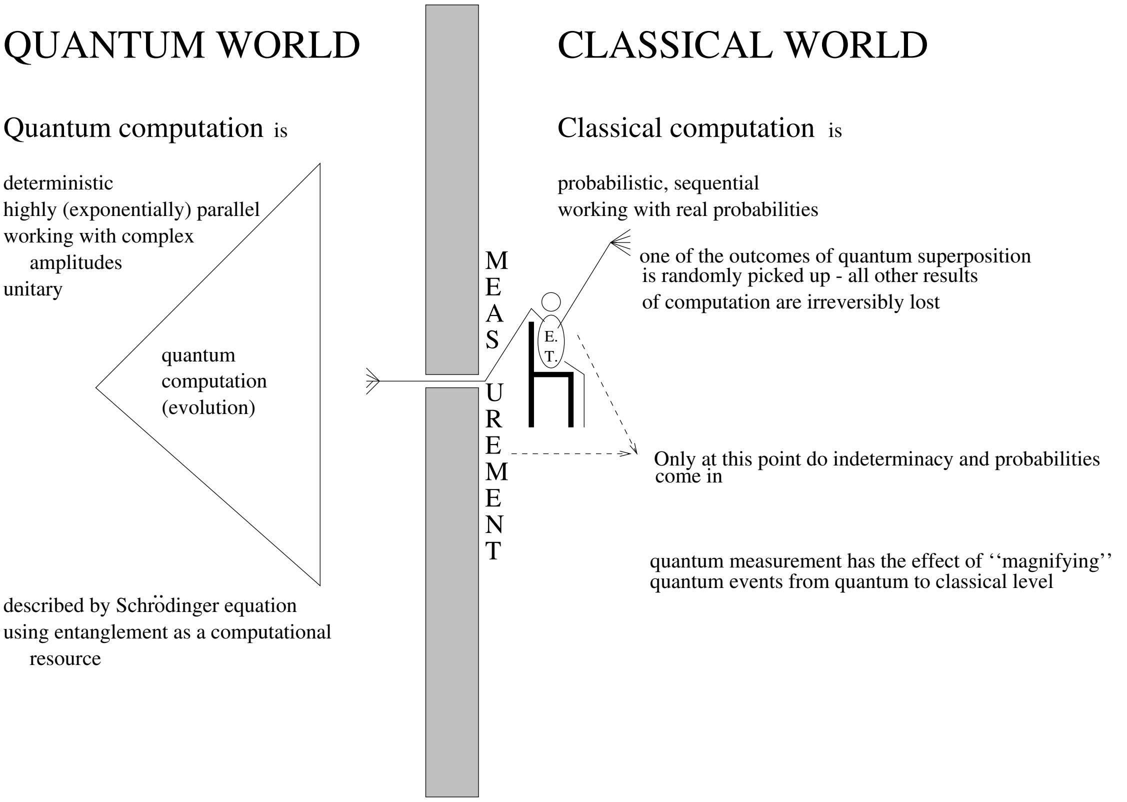
Jozef Gruska

Faculty of Informatics
Brno
Czech Republik

March 25, 2000

QUANTUM COMPUTING

Jozef Gruska


QUANTUM WORLD
CLASSICAL WORLD
Quantum computation is
Classical computation is
deterministic
highly (exponentially) parallel
working with complex amplitudes
unitary
probabilistic, sequential
working with real probabilities
one of the outcomes of quantum superposition is randomly picked up - all other results of computation are irreversibly lost
quantum computation (evolution)
MEASUREMENT
E. T.
Only at this point do indeterminacy and probabilities come in
quantum measurement has the effect of ''magnifying'' quantum events from quantum to classical level
described by Schrödinger equation
using entanglement as a computational resource

ABSTRACT

In quantum computing we witness a merge of two of the most important areas of science of 20th century: quantum physics and informatics.

This merge is bringing new aims, challenges and potentials for informatics and also new approaches to explore quantum world.

In spite of the fact that it is hard to predict particular impacts of quantum computing on computing in general, it is quite safe to expect that the merge will lead to important outcomes.

In the lecture the very basic aims, history, principles, concepts, models, methods, results, as well as problems of quantum computing will be presented with emphasis much more on computational aspects than on the underlying physics.

1. INTRODUCTION

In the first lecture we deal with reasons why to study quantum computing and with very basic experiments, principles and formalism of quantum mechanics.

We deal also, in some details, with classical reversible computations, as a special case of quantum computation.

In quantum computing we witness an interaction between the two most important areas of science and technology of 20-th century, between

quantum physics and **informatics**.

This may have important consequences for 21st century.

QUANTUM PHYSICS

is

is an **excellent theory** to predict probabilities of quantum events.

Quantum physics is an elegant and conceptually simple theory that describes with astounding precision a large spectrum of the phenomena of Nature.

The predictions made on the base of quantum physics have been experimentally verified to 14 orders of precision. No conflict between predictions of theory and experiments is known.

Without quantum physics we cannot explain properties of superfluids, functioning of laser, the substance of chemistry, the structure and function of DNA, the existence and behaviour of solid bodies, color of stars, ...

QUANTUM PHYSICS — SUBJECT

Quantum physics deals with fundamentals entities of physics — particles like

- protons, electrons and neutrons (from which matter is built);
- photons (which carry electromagnetic radiation);
- various "elementary particles" which mediate other interactions of physics.

We call them **particles** in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary world.

Indeed, it is not clear in what sense these "particles" can be said to have properties at all.

You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything

Bernard Shaw (1938)

WHAT QUANTUM PHYSICS TELL US?

Quantum physics

tells us

WHAT happens

but does not tell us

WHY it happens

and does not tell us either

HOW it happens

WHAT QUANTUM PHYSICS TELLS US?

- Quantum physics tells us that things do not behave at the quantum (particle or microscopic) level the way we are used to in our macroscopic experience.
- Quantum physics also tells us **what** happens at the quantum level, but it does not tell us neither **why** it happens nor **how** it happens.

QUANTUM PHYSICS

is, from the point of view of explaining quantum phenomena, a very unsatisfactory theory.

Quantum physics is a theory with either some hard to accept principles or a theory leading to mysteries and paradoxes.

> *Quantum theory sems to lead to philosophical standpoints that many find deeply unsatisfying.*
> *At best, and taking its descriptions at their most literal, it provides us with a very strange view of the world indeed.*
> *At worst, and taking literally the proclamations of some of its most famous protagonists, it provides us with no view of the world at all.*
>
> Roger Penrose

QUANTUM PHYSICS VIEWS

Quantum physics, that mysterious, confusing discipline, which none of us really understands, but which we all know how to use.

M. Gell-Mann

Physical concepts are free creations of the human min, and are not, however it may seem, uniquely determined by the external world.

Albert Einstein

QUANTUM PHYSICS UNDERSTANDING

I am going to tell you what Nature behaves like......

However do not keep saying to yourself, if you can possibly avoid it,

BUT HOW CAN IT BE LIKE THAT?

because you will get "down the drain" into a blind alley from which nobody has yet escaped.

NOBODY KNOWS HOW IT CAN BE LIKE THAT.

Richard Feynman (1965): The character of physical law.

WHY QUANTUM COMPUTING?

1. **Quantum computing** is a natural **challenge** because the world we live in is quantum mechanical.
2. **Quantum computing** seems to be in some sense a **necessity**.
3. **Quantum computing** seems to have **potential** to be essentially faster than classical computing for solving some important algorithmic problems.
4. **Research in quantum computing** seems to have potential to contribute to the essential increase of our knowledge about the world we live in.
5. For modern cryptography even the vision that a powerful quantum computer may exist in 20-30 years represents a significant danger for safety of current cryptographic communications and signatures.

PERFORMANCE OF PROCESSORS

1. There are no reasons why the increase of performance of processors should not follow **Moore law** in the near future.
2. A long term increase of performance of processors according to **Moore law** seems to be possible only if, at the performance of computational processes, we get more and more on atomic level.

EXAMPLE

A curve depicting the number of electrons needed to store a bit of information.
An interpolation of the curve indicates that we should compute soon at atomic level.

MOORE LAW

On the base of quantum mechanics one can determine that "ultimate laptop" of mass 1 kg and size 1 l cannot perform more than 2.7×10^{50} bit operations per second.

Calculations (Lloyd, 1999), are based only on the amount of energy needed to switch from one state to another distinguishable state.

It seems to be harder to determine the number of bits of such an "ultimate laptop". However, the bound 3.8×10^{16} has been determined for a computer compressed to form a black hole.

It is clear that Moore law cannot hold longer than for another 200 years.

CLASSICAL versus QUANTUM COMPUTING

The essence of the difference
between
classical computers and **quantum computers**

is in the way information is stored and processed.

In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

$$0 \quad \text{or} \quad 1$$

In **quantum computers**, information is represented on **microscopic level** using **qubits**, which can take on any from uncountable many values

$$\alpha|0\rangle + \beta|1\rangle$$

where α, β are arbitrary complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1.$$

A VISION of a QUANTUM COMPUTER

Imagine a computer

- memory of which is exponentially larger than its apparent physical size;
- which can process exponentially many data in one step;
- which computes in twilight zone of Hilbert space,

and you will see a quantum computer.

PRE-HISTORY

1970 Landauer demonstrated importance of reversibility for minimal energy computation;

1973 Bennett showed the existence of universal reversible Turing machines;

1981 Toffoli-Fredkin designed a universal reversible gate for Boolean logic;

1982 Benioff showed that quantum processes are at least as powerful as Turing machines;

1982 Feynman demonstrated that quntum physics cannot be simulated effectively on classical computers;

1985 Deutsch showed the existence of a universal quantum Turing machine.

1993 Bernstein-Vazirani-Yao showed the existence of an efficient universal quantum Turing machine;

1994 Shor discovered a polynomial time quantum algorithm for factorization;

1994 Quantum cryptography went through an experimental stage;

1995 DiVincenzo designed a universal gate with two inputs and outputs;

1995 Cirac and Zoller demonstrated a chance to build quantum computers using existing technologies.

REVERSIBILITY

QUANTUM PROCESSES ARE REVERSIBLE

An operation is reversible if its outputs uniquely determine its inputs.

$$(a, b) \rightarrow a + b$$

a non-reversible operation

$$(a, b) \rightarrow (a + b, a - b)$$

a reversible operation

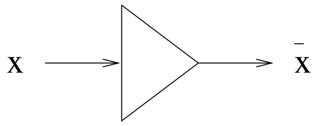
$$a \rightarrow f(a)$$

A mapping that can but does not have to be reversible

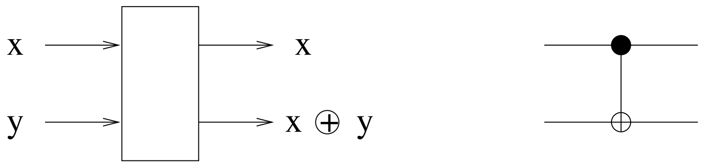
$$(a, 0) \rightarrow (a, f(a))$$

a surely reversible operation

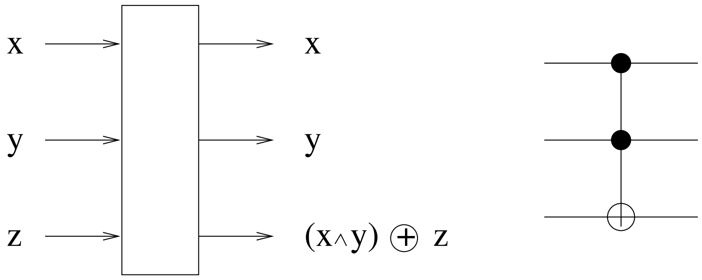
REVERSIBLE GATES



NOT-gate



CNOT = XOR-gate



CCNOT-gate

A universal reversible gate for
Boolean logic

Three reversible classical gates: NOT gate, XOR or CNOT gate and Toffoli or CCNOT gate.

GARBAGE REMOVAL

In order to produce reversible computation one needs to produce garbage (information). Its removal is possible and important.

Bennett (1973) has shown that if a function f is computable by a one-tape Turing machine in time $t(n)$, then there is a 3-tape reversible Turing machine computing, with constant time overhead, the mapping

$$a \to (a, g(a), f(a))$$

Bennett (1973) has also shown that there is an elegant reversible way how to remove garbage:

Basic computation: of f: $a \to (a, g(a), f(a))$.

Fanout: $(a, g(a), f(a)) \to (a, g(a), f(a), f(a))$

Uncomputing of f : $(a, g(a), f(a), f(a)) \to (a, f(a))$

THREE BASIC PRINCIPLES

P1 To each transfer from a quantum state ϕ to a state ψ a complex number

$$\langle\psi|\phi\rangle$$

is associated, which is called the **probability amplitude** of the transfer, such that

$$|\langle\psi|\phi\rangle|^2$$

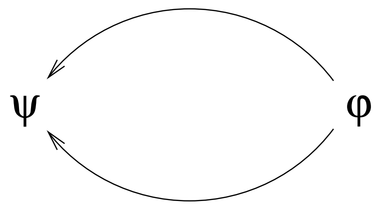
is the **probability** of the transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers

$$\psi \leftarrow \phi' \leftarrow \phi$$

then the resulting amplitude of the transfer is the **product** of amplitudes of subtransfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from a state ϕ to a state ψ has two independent alternatives



then the resulting amplitude is the sum of amplitudes of two subtransfers.

CLASSICAL EXPERIMENTS

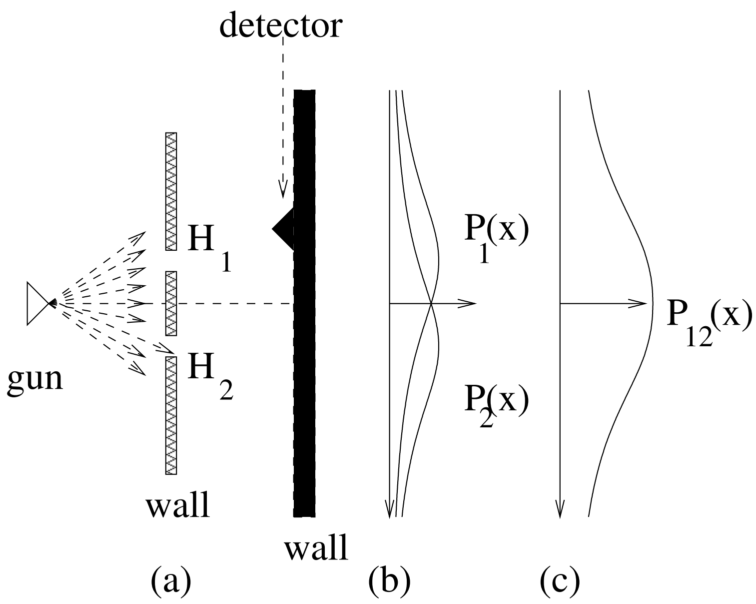


Figure 1: Experiment with bullets

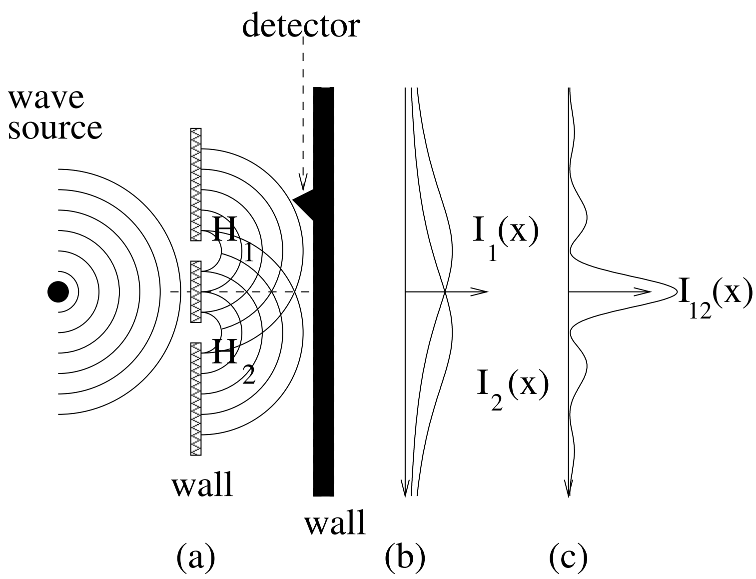


Figure 2: Experiments with waves

QUANTUM EXPERIMENTS

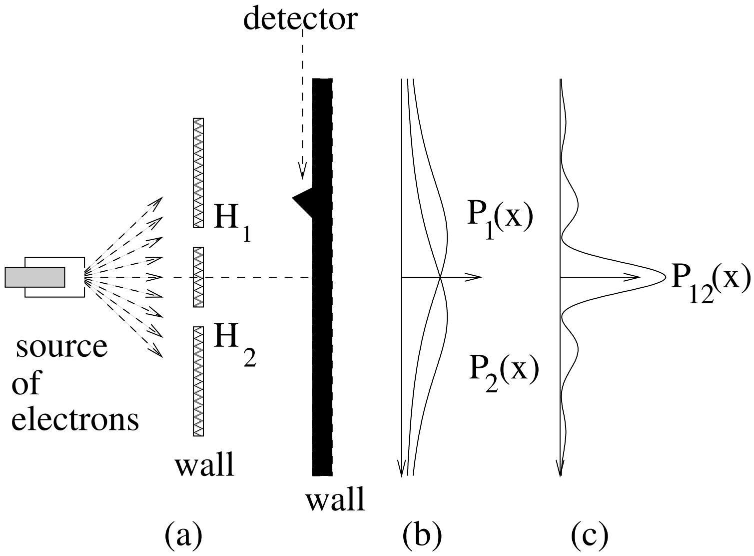


Figure 3: Two-slit experiment

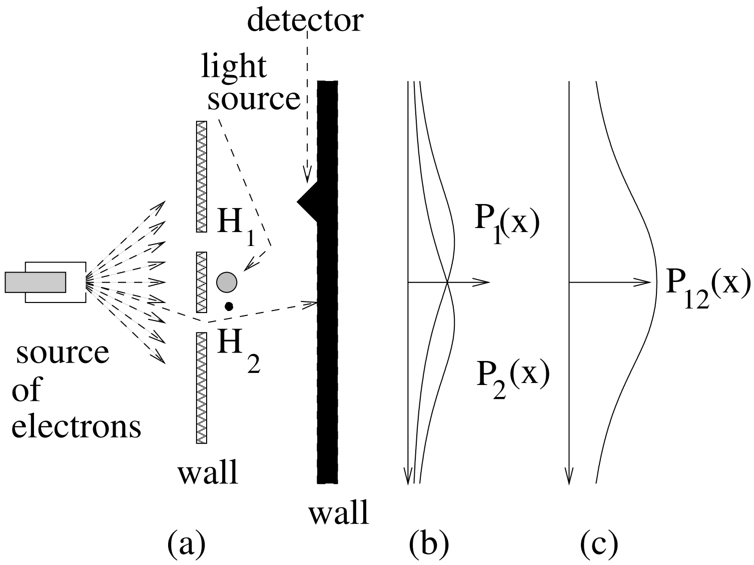


Figure 4: Two-slit experiment with an observation

TWO-SLIT EXPERIMENT – OBSERVATIONS

- Contrary to our intuition, at some places one observes fewer electrons when both slits are open, than in the case only one slit is open.
- Electrons — particles, seem to behave as waves.
- Each electron seems to behave as going through both holes at once.
- Results of the experiment do not depend on frequency with which electrons are shot.
- Quantum physics has no explanation where a particular electron reaches the detector wall. All quantum physics can offer are statements on the probability that an electron reaches a certain position on the detector wall.

QUANTUM EVOLUTION/COMPUTATION

EVOLUTION	COMPUTATION
in	in
QUANTUM SYSTEM	HILBERT SPACE

is described by

Schrödinger linear equation

$$i\hbar\frac{\partial\psi(t)}{\partial t} = H(t)\psi(t)$$

from which it follows that evolution (computation) of a quantum system is performed by a **unitary operator** and a step of such an evolution we can see as a multiplication of a **unitary matrix** A with a vector $|\psi\rangle$, i.e.

$$A|\psi\rangle$$

A matrix A is **unitary** if

$$A \cdot A^{*} = A^{*} \cdot A = I$$

UNITARY MATRICES — EXAMPLES

In the following figure there are examples of unitary matrices of degree 2

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(a) (b) (c)

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$$

(d) (e)

$$\begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix} \quad \begin{pmatrix} e^{i\alpha}\cos\theta & -ie^{i(\alpha-\theta)}\sin\theta \\ -ie^{i(\alpha+\theta)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix}$$

(f) (g)

Figure 5: Examples of unitary matrices of degree 2

Matrices σ_x, σ_y and σ_z are so called **Pauli matrices**. They play an important role in quantum computing and have the following interesting important properties.

- Unitary matrix I of degree 2 and Pauli matrices form a basis of all matrices of degree 2. That is each matrix of degree two can be expressed as a linear combination of these matrices.
- Pauli matrices have the following properties: (a) $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$; (b) $\sigma_k\sigma_l = i\sigma_m$, where (k,l,m) is a cyclic permutation of (x,y,z); (c) all Pauli matrices have eigenvalues 1 and -1.

UNITARITY OF MATRICES

A matrix A is unitary if

$$AA^* = I = A^*A$$

If the matrix A is finite then

$$AA^* = 1 \Longleftrightarrow A^*A = I$$

The above equivalence does not have to be true if the matrix¡A is infinite. Example:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & \dots & \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Observe that equality $AA^* = 1$ is equivalent to the statement that row of A are orthogonal.

Unitarity of a matrix therefore implies that its rows (columns) are orthogonal.

QUANTUM SYSTEMS

=

HILBERT SPACE

Hilbert space H_n is n-dimensional complex vector space with

scalar product

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \quad \text{of vectors } |\phi\rangle = \left| \begin{array}{c} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{array} \right|, |\psi\rangle = \left| \begin{array}{c} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{array} \right|,$$

norm of vectors

$$||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$$

and the **metric**

$$\text{dist}(\phi, \psi) = ||\phi - \psi||.$$

This allows us to introduce on H a metric topology and such concepts as continuity.
For each ϕ of a Hilbert space H the mapping $f_\phi : H \rightarrow \mathbf{C}$ defined by

$$f_\phi(\psi) = \langle\phi|\psi\rangle$$

is a linear mapping on H in the sense that $f_\phi(c\psi) = cf_\phi(\psi)$ and $f_\phi(\psi_1 + \psi_2) = f_\phi(\psi_1) + f_\phi(\psi_2)$. One can even show that we get all linear mappings from H to $\mathbf{C}$ by this construction. Namely, it holds:

Theorem To each continuous linear mapping $f : H \rightarrow \mathbf{C}$ there exists a unique $\phi_f \in H$ such that $f(\psi) = \langle\phi_f|\psi\rangle$ for any $\psi \in H$.

$\boxed{\text{MYSTERIOUS WARNING}}$

A quantum system is a useful abstraction which frequently appears in the literature, but does not really exists in nature.

A. Peres (1993)

BRA-KET NOTATION

Dirack introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals $f : H \to \mathbf{C}$.

If $\psi, \phi \in H$, then

$\langle\psi|\phi\rangle$ — scalar product of ψ and ϕ
(an amplitude of going from ϕ to ψ).

$|\phi\rangle$ — **ket-vector** — an equivalent to ϕ

$\langle\psi|$ — **bra-vector** a linear functional on H
such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$

QUBITS

A **qubit** is a quantum state in H_2

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and

$$\{|0\rangle, |1\rangle\} \quad \text{is a } \textbf{(standard) basis} \text{ of } H_2$$

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

(b) a spin-$\frac{1}{2}$ particle

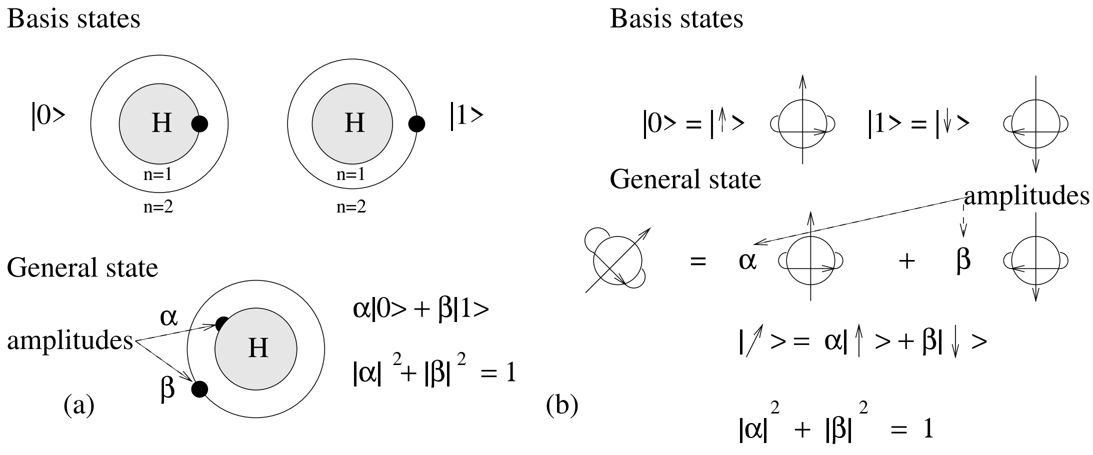


Figure 6: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

x

ORTHOGONALITY of STATES

Two vectors $|\phi\rangle$ and $|\psi\rangle$ are called **orthogonal** if $\langle\phi|\psi\rangle = 0$. Physically are fully distinguishable only orthogonal vectors (states).

A **basis** $\mathcal{B}$ of H_n is any set of n vectors $|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle$ of the norm 1 which are orthogonal.

Given a basis $\mathcal{B}$, any vector $|\psi\rangle$ from H_n can be uniquely expressed in the form

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle.$$

A set S of vectors is called **orthonormal** if all vectors of S have norm 1 and are nutually orthogonal.

Definition A **subspace** G of a Hilbert space H is a subset of H closed under addition and scalar multiplication.

An important property of Hilbert spaces is their decomposability into mutually orthogonal subspaces. It holds:

Theorem For each closed subspace W of a Hilbert space H there exists a unique subspace $W^{\perp}$ such that $\langle\phi|\psi\rangle = 0$, whenever $\phi \in W$ and $\psi \in W^{\perp}$ and each $\psi \in H$ can be uniquely expressed in the form $\psi = \phi_1 + \phi_2$, with $\phi_1 \in W$ and $\phi_2 \in W^{\perp}$. In such a case we write $H = W \oplus W^{\perp}$ and we say that W and $W^{\perp}$ form an orthogonal decomposition of H.

In a natural way we can make a generalization of an orthogonal decomposition

$$H = W_1 \oplus W_2 \oplus \ldots \oplus W_n,$$

of H into mutually orthogonal subspaces $W_1, \ldots, W_n$ such that each $\psi \in H$ has a unique representation as $\psi = \phi_1 + \phi_2 + \ldots + \phi_n$, with $\phi_i \in W_i, 1 \leq i \leq n$.

OPERATORS of HILBERT SPACES

A linear operator on a Hilbert space H is a linear mapping $A : H \rightarrow H$.

An application of a linear operator A to a vector $|\psi\rangle$ is denoted $A|\psi\rangle$.

A is also a linear operator of the dual Hilbert space H^*, mapping each linear functional $\langle\phi|$ of the dual space to the linear functional, denoted by $\langle\phi|A$.

A linear operator A is called **positive** or **semi-definite**, notation $A \geq 0$, if $\langle\psi|A\psi\rangle \geq 0$ for every $|\psi\rangle \in H$.

Each linear operator A of a countable Hilbert space H with a basis $\mathcal{B} = \{|\theta_i\rangle \,|\, i \in I\}$ can be represented by a matrix, in general infinitely dimensional, whose rows and columns are labeled by elements of I and with $\langle\theta_i|A|\theta_j\rangle = \langle\theta_i|A\theta_j\rangle$ in the i-th row and j-th column.

The **norm** $||A||$ of a linear operator A is defined as

$$||A|| = \sup_{||\phi||=1} ||A|\phi\rangle||.$$

A linear operator A is called **bounded** if its norm $||A||$ is finite.

Projections have a special role among linear operators.

If $H = W_1 \oplus W_2$ is an orthogonal decomposition of a Hilbert space H into subspaces W_1 and W_2, then, as mentioned above, each $\psi \in H$ has a unique representation $\psi = \psi_1 + \psi_2$, where $\psi_1 \in W_1$ and $\psi_2 \in W_2$.

$$P_{W_1}(\psi) = \psi_1 \quad \text{and} \quad P_{W_2}(\psi) = \psi_2$$

are called **projections** onto the subspaces W_1 and W_2, respectively.

SELF-ADJOINT OPERATOS — HERMITIAN MATRICES

To self-adjoint operators correspond **Hermitian matrices**, i.e., matrices A such that $A = A^*$.

Theorem 0.1 *Hermitian matrices have the following properties.*

1. *All eigenvalues of a Hermitian matrix are real.*
2. *The determinant of a Hermitian matrix equals the product of its eigenvalues.*
3. *The* **trace** *(the sum of diagonal elements) of a Hermitian matrix A, notation* Tr(A)*, equals the sum of its eigenvalues .*

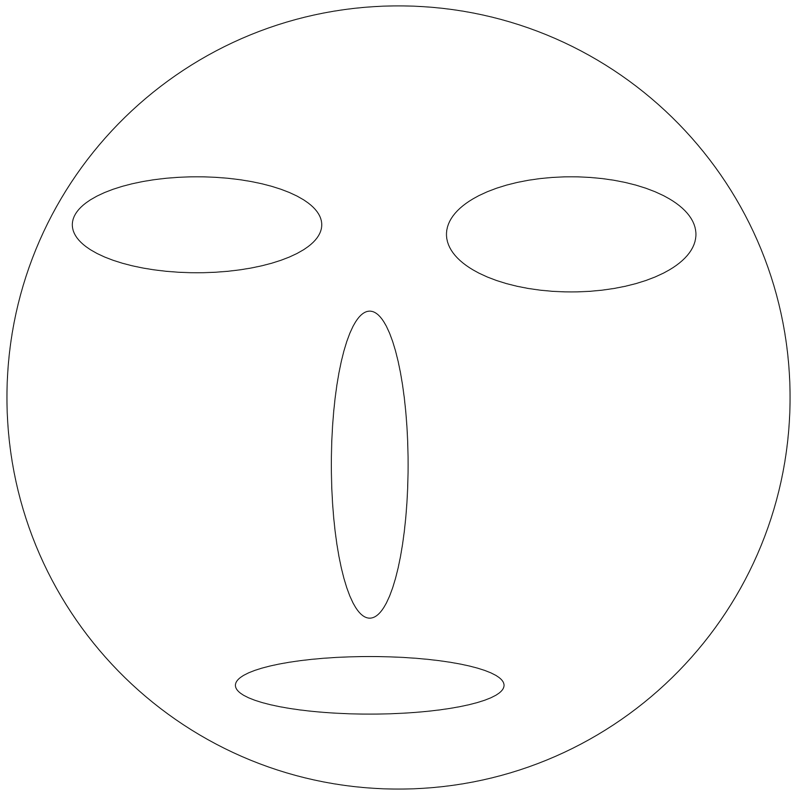
A self-adjoint operator A of a finite dimensional Hilbert space H has the so-called **spectral representation**. If $\lambda_1, \ldots, \lambda_k$ are its distinct eigenvalues, then A can be expressed in the form

$$A = \sum_{i=1}^{k} \lambda_i P_i,$$

where P_i is the projection operator into the subspace of H spanned by the eigenvectors corresponding to λ_i.

QUANTUM (PROJECTION) MEASUREMENTS

A quantum state is observed (measured) with respect to an **observable** — a decomposition of a given Hilbert space into orthogonal subspaces (such that each vector can be uniquely represented as a sum of vectors of these subspaces).



There are two outcomes of a projection measurement of a state $|\phi\rangle$:

1. Information into which subspace projection of $|\phi\rangle$ was made.
2. Resulting projection (a new state) $|\phi'\rangle$.

The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ at the basis states of the subspace.

STERN-GERLACH MEASUREMENT EXPERIMENT

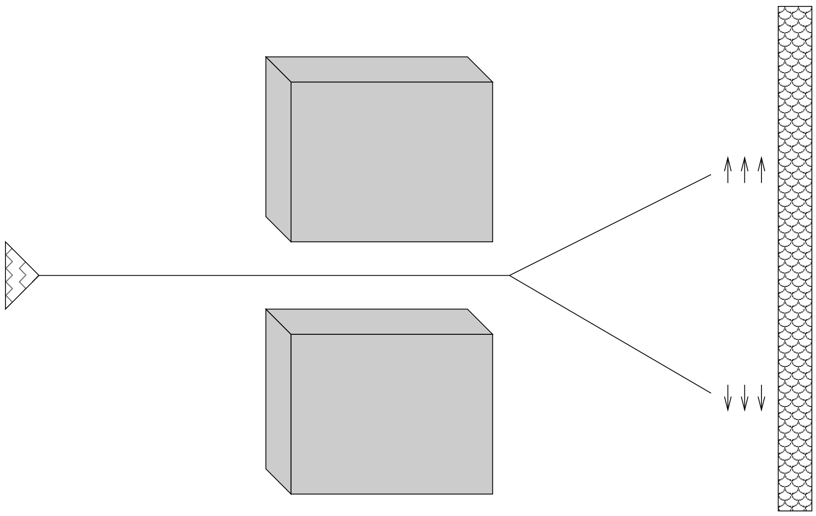


Figure 7: Stern-Gerlach experiment with spin-$\frac{1}{2}$ particles

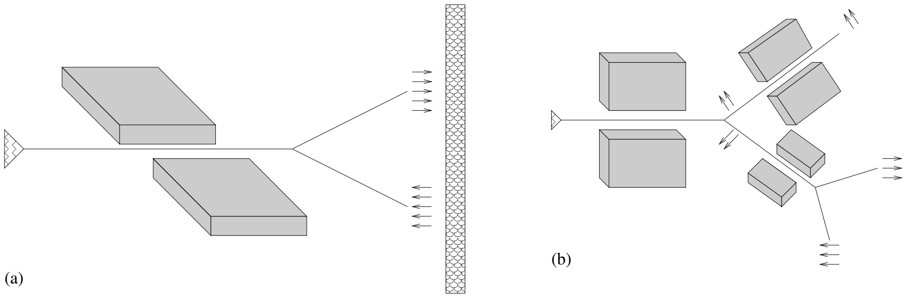


Figure 8: Several Stern-Gerlach magnets

$\boxed{\text{MEASUREMENT}}$

in CLASSICAL versus QUANTUM physics

BEFORE QUANTUM PHYSICS

it was taken for granted that when physicists measure something, they are gaining knowledge of a pre-existing state — a knowledge of an independent fact about the world.

QUANTUM PHYSICS

says otherwise. Things are not determined except when they are measured, and it is only by being measured that they take on specific values.

A quantum measurement forces a previously indeterminate system to take on a definite value.

TENSOR PRODUCTS

of vectors

$$(x_1,\ldots,x_n)\otimes(y_1,\ldots,y_m)=(x_1y_1,\ldots,x_1y_m,x_2y_1,\ldots,x_2y_m,\ldots,x_ny_1,\ldots,x_ny_m)$$

of matrices $$A\otimes B=\begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \ldots & a_{nn}B \end{pmatrix}$$

where $$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & & \ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\otimes\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\otimes\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix}$$

of Hilbert spaces $H_1 \otimes H_2$ is the complex vector space spanned by tensor products of vectors from H_1 and H_2, that corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces H_1 and H_2.

An important difference between classical and quantum systems

A state of a compound classical (quantum) system can be (cannot be) always composed from the states of the subsystems.

DENSITY MATRICES

Let a quantum source X produces quantum states $\{|\phi_i\rangle\}_{i=1}^n$, and the state $|\phi_i\rangle$ with probability p_i

$$[\phi\rangle = \bigoplus_{i=1}^{n}(p_i, |\phi_i\rangle)$$

is called **mixed state** of X and

$$\rho_X = \sum_{i=1}^{n} p_i|\phi_i\rangle\langle\phi_i|$$

is its **density matrix**

IMPORTANT OBSERVATION. Two mixed states with the same density matrix are physically not distinguishable.

Example For the mixed state:

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

and, for any qubit state $\alpha|0\rangle + \beta|1\rangle$,

$$(\frac{1}{4}(-\alpha|0\rangle - \beta|1\rangle), \frac{1}{4}(-\alpha|0\rangle + \beta|1\rangle), \frac{1}{4}(\beta|0\rangle + \alpha|1\rangle), \frac{1}{4}(-\beta|0\rangle + \alpha|1\rangle))$$

have the same density matrix, namely $\frac{1}{2}I$.

SUPEROPERATORS

The most general operators on density matrices (and quantum (mixed) states) are so-called **superoperators**.

Informally, the best way is to see a superoperator S applied to a state $|\phi\rangle$ of a Hilbert space H as to take first an auxiliary state (called usually **ancilla**) of another Hilbert space H', then to apply a unitary operator U to the state $|\phi\rangle \otimes |\psi\rangle$ and, finally, to discard the H'-part of the resulting state.

Formally, a superoperator is a certain positive trace preserving linear transformation over density matrices.

Examples of superoperators are: quantum noisy channel, encoders and decoders.

REVERSIBLE TWO-BIT ADDER

Example 0.2 *The two bit adder computation mapping:*

$$(a, b) \rightarrow (a \oplus b, a \wedge b) \qquad \{\textit{(sum, carry)}\}$$

is not one-to-one. However, the modified computational task:

$$(a, b) \rightarrow (a, a \oplus b, a \wedge b)$$

is a one-to-one mapping and can be realized using one CN gate and one CCN gate, with the constant input $c = 0$*, as shown in Figure 9.*

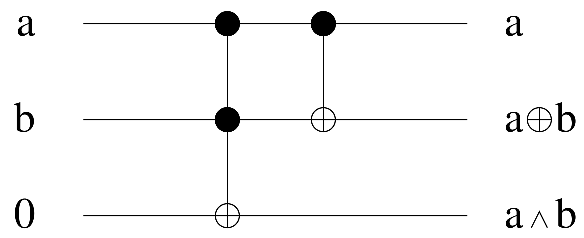


Figure 9: A reversible implementation of a two-bit adder

BILLIARD BALL REVERSIBLE COMPUTER

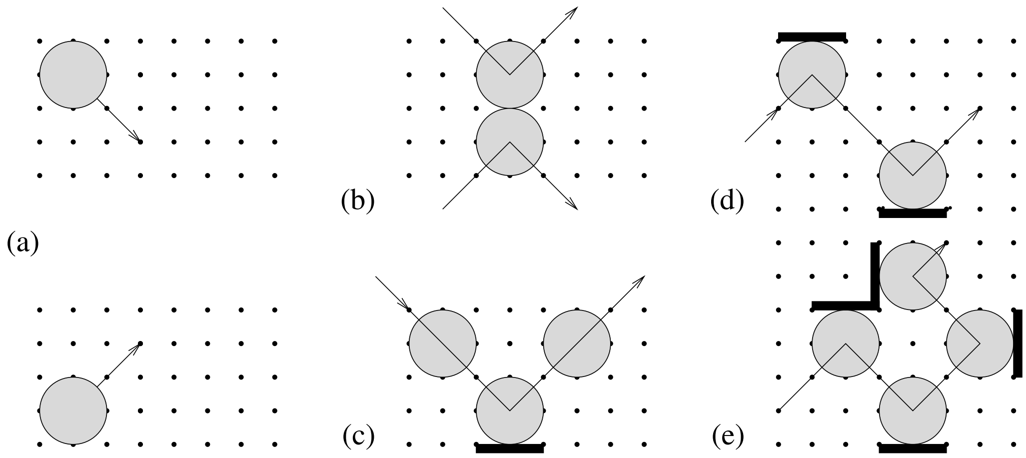


Figure 10: Billiard ball model of reversible computation

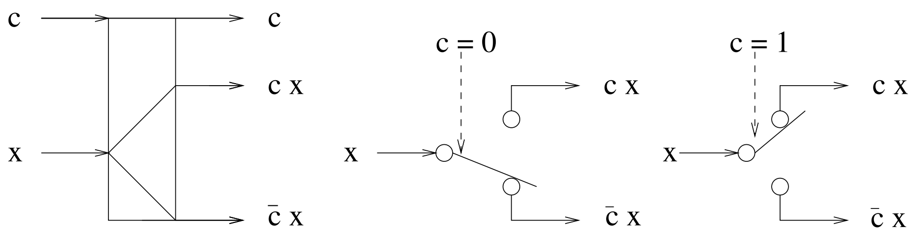


Figure 11: Switch gate

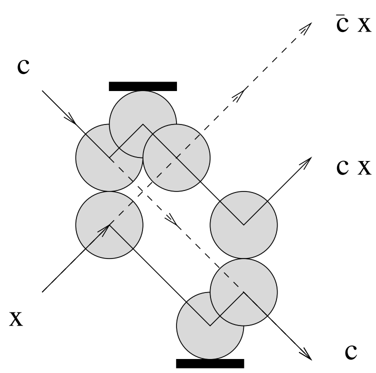


Figure 12: A billiard ball implementation of the switch gate