INTRODUCTION TO QUANTUM COMPUTATION, COMMUNICATION AND SECURITY

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

October 13, 2020

PROLOGUE - I.

- The idea to build a quantum computer has emerged around 1982.
- Around 1996 it started to be quite clear that that we can consider such an idea as feasible.
- For years researchers were able to build quantum processors only with less than 10 qubits.
- Recently situation has started to change.
- In 2016 Intel has design a 49 qubits processor.
- In 2017 IBM announced a 50 qubits processor.
- In May 2018 Google announced a 72 qubits processor.

PROLOGUE - II.

- In 2007 Canadian company D-WAVE announced 16 qubits ”quantum computer” D-Wave
- As the next step they announced 28 qubits quantum computer D-Wave
- As the next step they announced a 128 qubits computer D-Wave
- As the next step they announced a 512 qubits D-wave computer
- In 2008 they announced a 1024 qubits D-wave computer
- In 2018 they announced a 2000 qubits D-wave computer

However, view differ how are these computers inherently quantum.

PROLOGUE

Progress in quantum key distribution:

- First experimental key distribution for 38 cm , 1989
- 10km fiber key distribution, 1994
- 67km fiber key distribution, under Geneva lake, 2002
- 1.8 km free space quantum key distribution
- 141 km free space quantum key distribution, Canary islands, 2007
- 120 km quantum key distribution on fiber, 2016
- 2000 km satellite quantum key distribution, 2018
- Underwater quantum key distribution, 2014

Chapter 1. INTRODUCTION - WHY QUANTUM COMPUTA

In the first lecture we present and discuss at first main reasons why quantum information processing, communication and security are new and very interesting ideas for information processing in general and for computing, communication and security in particular. Secondly we present and analyze very basic experiments, that were behind e developments and theoretical capturing quantum mechanics as one of the basic theory of physical and also nformation processing worlds.

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

INTRODUCTORY OBSERVATIONS

-

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.

INTRODUCTORY OBSERVATIONS

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.

A VIEW of HISTORY

19th century was mainly influenced by the first industrial revolution that had its basis in the classical mechanics discovered, formalized and developed in the 18th century.

20th century was mainly influenced by the second industrial revolution that had its basis in electrodynamics discovered, formalized and developed in the 19th century.

21th century can be expected to be mainly developed by quantum mechanics and informatics discovered, formalized and developed in the 20th century.

FROM CLASSICAL to QUANTUM PHYSICS

At the end of 19th century it was believed by most that the laws of Newton and Maxwell were correct and complete laws of physics.

At the beginning of 20th century it got clear that these laws are not sufficient to explain all observed physical phenomena.

As a result, a new mathematical framework for physics called *quantum mechanics* was formulated and a new theory of physics, called *quantum physics* was developed.

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) - they are the only particles we can directly observe;
- 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.

QUANTUM MECHANICS - ANOTHER VIEW

- Quantum mechanics is not physics in the usual sense - it is not about matter, or energy or waves, or particles - it is about information, probabilities, probability amplitudes and observables, and how they relate to each other.
- Quantum mechanics is what you would inevitably come up with if you would started from probability theory, and then said, let’s try to generalize it so that the numbers we used to call ”probabilities” can be negative numbers.

  As such, the theory could be invented by mathematicians in the 19th century without any input from experiment. It was not, but it could have been (Aaronson, 1997).

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

nor

HOW MUCH it costs

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 nor how much it costs.**

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 seems 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.

QUANTUM MECHANICS

Quantum physics phenomena are difficult to understand since at attempts to understand quantum physics most of our everyday experiences are not applicable.

Quantum mechanics is a theory in mathematical sense: it is governed by a set of axioms.

MATHEMATICS BEHIND QUANTUM MECHANICS

- **Concerning mathematics behind quantum mechanics, one should actually do not try to understand what mathematics means, one should try to learn to work with it.**
- **Nobody saw superposition of quantum states - one can ”see” only a basis state.**

QUANTUM PHYSICS - OBSERVATION

It is well known that it is very hard to understand quantum physics

however,

it is less known that understanding of quantum physics is child's play comparing with understanding of child's play.

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.

WHY is QIPC so IMPORTANT?

There are five main reasons why QIPC is increasingly considered as of (very) large importance:

- QIPC is believed to lead to new Quantum Information Processing Technology that could have deep and broad impacts.
- Several areas of science and technology are approaching the point at which they badly need expertise with isolation, manipulating and transmission of particles.
- It is increasingly believed that new, quantum information processing based, understanding of (complex) quantum phenomena and systems can be developed.
- Quantum cryptography seems to offer new level of security and be soon feasible.
- QIPC has been shown to be more efficient in interesting/important cases.
- TCS and Information theory got new dimension and impulses.

WHY von NEUMANN

DID (COULD) NOT DISCOVER QUANTUM COMPUTING?

- **No computational complexity theory was known (and needed).**
- **Information theory was not yet well developed.**
- **Progress in physics and technology was far from what would be needed to make even rudimentary implementations.**
- **The concept of randomized algorithms was not known.**
- **No public key cryptography was known (and needed).**

WHEN WE CAN EXPECT to have powerful QUANTUM CO

- Recently, NSA announced that it plans to shift the encryption of governmental and military data away from current cryptographic schemes to new ones, yet to be determined, that could resist any attack by quantum computers.
- The reason behind is that NSA expect that powerful quantum computers will be available within 5-30 years.

DEVELOPMENT of BASIC VIEWS

on the role of information in physics:

- Information is information, nor matter, nor energy.

  Norbert Wiener

- Information is physical

  Ralf Landauer

  Should therefore information theory and foundations of computing (complexity theory and computability theory) be a part of physics?

- Physics is informational

  Should (Hilbert space) quantum mechanics be a part of Informatics?

WHEELER's VIEW

I think of my lifetime in physics as divided into three periods

- In the first period ...I was convinced that
  EVERYTHING IS PARTICLE
- I call my second period
  EVERYTHING IS FIELDS
- Now I have new vision, namely that
  EVERYTHING IS INFORMATION

WHEELER's "IT from BIT"

IT FROM BIT symbolizes the idea that every item of the physical world has at the bottom - at the very bottom, in most instances - an immaterial source and explanation.

Namely, that which we call reality arises from posing many yes-no questions, and registering of equipment-invoked responses.

In short, that things physical are information theoretic in origin.

MAIN PARADOX

- Quantum physics is extremely elaborated theory, full of paradoxes and mysteries. It takes any excellent physicist years to develop a proper feeling for quantum mechanics - for a proper relation between theory and physical reality.
- Some (theoretical) computer scientists/mathematicians, with almost no background in quantum physics, have been able to make crucial contributions to theory of quantum information processing.

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

An extrapolation of the curve depicting the number of electrons needed to store a bit of information shows that around 2020 we should need one electron to store one bit.

MOORE LAW

It is nowadays accepted that information processing technology has been developed for the last 50 years according the so-called Moore law. This law has now three forms.

Economic form: Computer power doubles, for constant cost, every two years or so.

Physical form: The number of atoms needed to represent one bit of information should halves every two years or so.

Quantum form: For certain application, quantum computers need to increase in the size only by one qubit every two years or so, in order to keep pace with the classical computers performance increase.

ULTIMATE LIMITS

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 quite 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

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

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 quantum physics cannot be simulated effectively on classical computers;

1984 Quantum cryptographic protocol BB84 was published, by Bennett and Brassard, for absolutely secure generation of shared secret random classical keys.

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

1989 First cryptographic experiment for transmission of photons, for distance 32.5cm was performed by Bennett, Brassard and Smolin.

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

1993 Quantum teleportation was discovered, by Bennett et al.

1994 Shor discovered a polynomial time quantum algorithm for factorization;

Cryptographic experiments were performed for the distance of 10km (using fibers).

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.

1995 Shor showed the existence of quantum error-correcting codes.

1996 The existence of quantum fault-tolerant computation was shown by Shor.

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

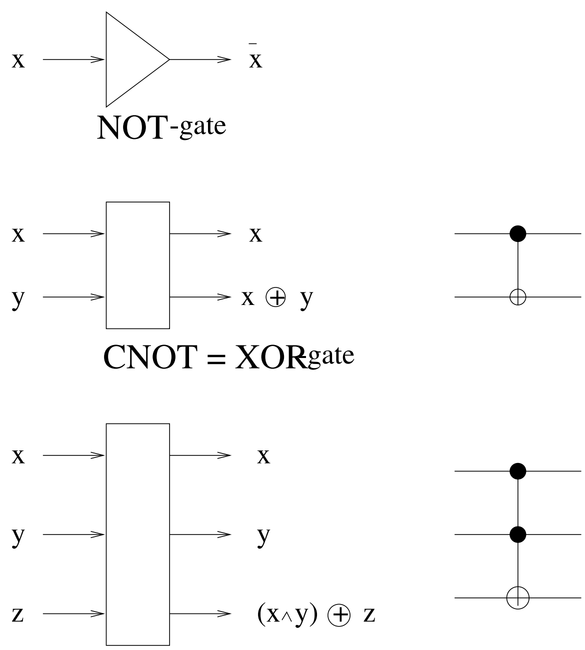
$a \rightarrow f(a)$

A mapping that can but does not have to be reversible

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

a surely reversible operation

REVERSIBLE GATES



CCNOT-gate

A universal reversible gate for Boolean logic

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

UNIVERSALITY of GATES

Definition A set $\mathcal{G}$ of gates is universal for classical computation if for any positive integers n, m and function $f : \{0,1\}^n \rightarrow \{0,1\}^m$, a circuit can be designed for computing f using only gates from $\mathcal{G}$.

Gates $\{$ NAND, FANOUT$\}$ form a universal set of gates.

The set consisting of just the Toffoli gate is also universal for classical computing (provided we add the ability to add ancillary bits to the circuit that can be initiated to either 0 or 1 as required).

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

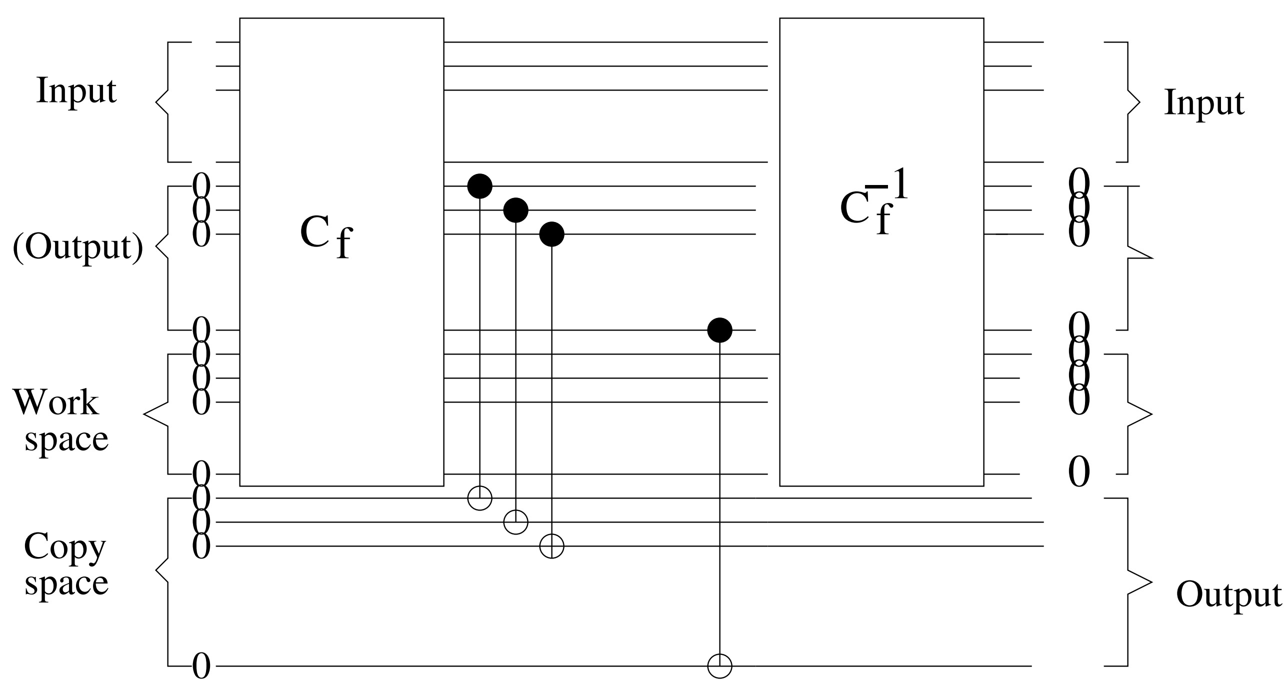
Uncomputing of f : $(a, g(a), f(a), f(a)) \to (a, f(a))$

CIRCUIT REPRESENTATION OF GARBAGE REMOVAL

Observe that CNOT gate with 0 as the initial value of the target bit is a copy gate. Indeed,

$$\text{CNOT}(x, 0) = (x, x)$$

A circuit version of the garbage removal has then the form



BILLIARD BALL REVERSIBLE COMPUTER

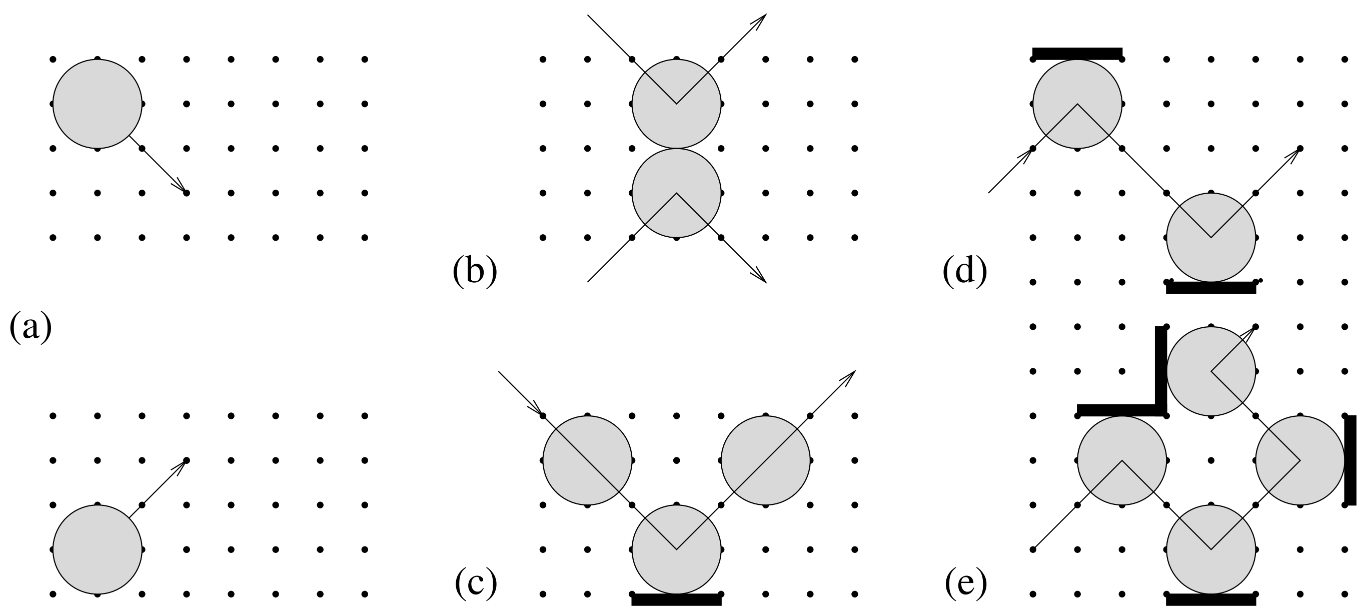


Figure 1: Billiard ball model of reversible computation

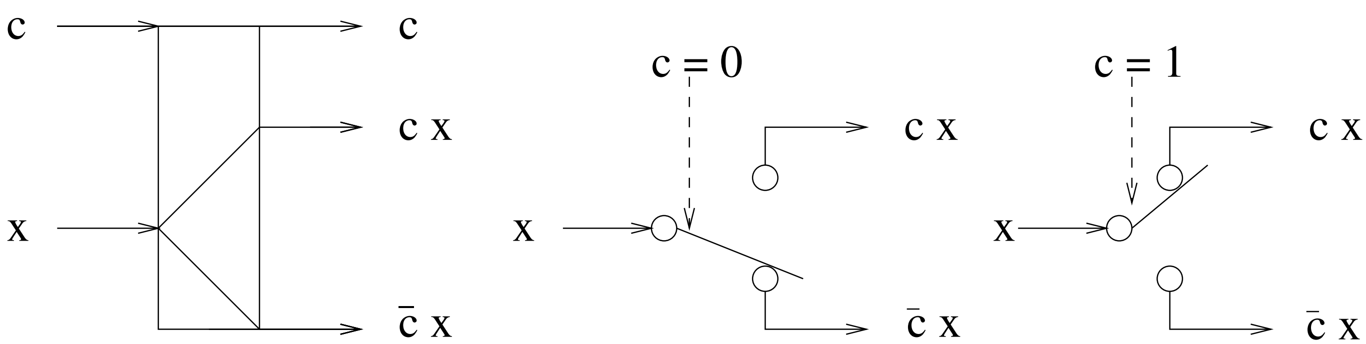


Figure 2: Switch gate

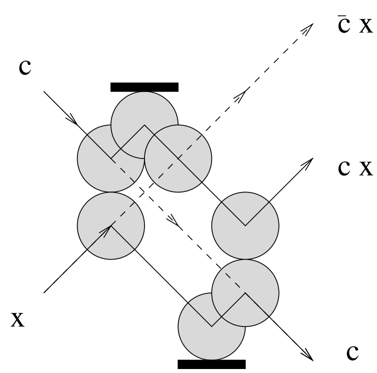


Figure 3: A billiard ball implementation of the switch gate

CLASSICAL EXPERIMENTS

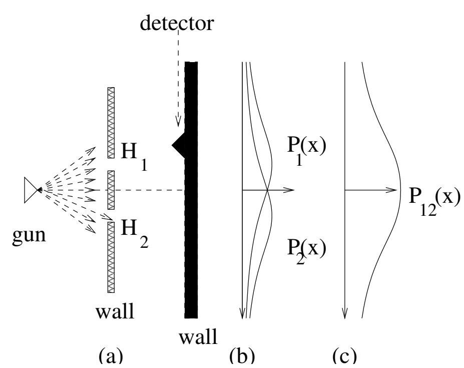


Figure 4: Experiment with bullets

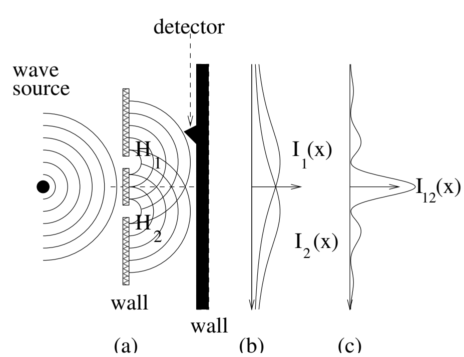


Figure 5: Experiments with waves

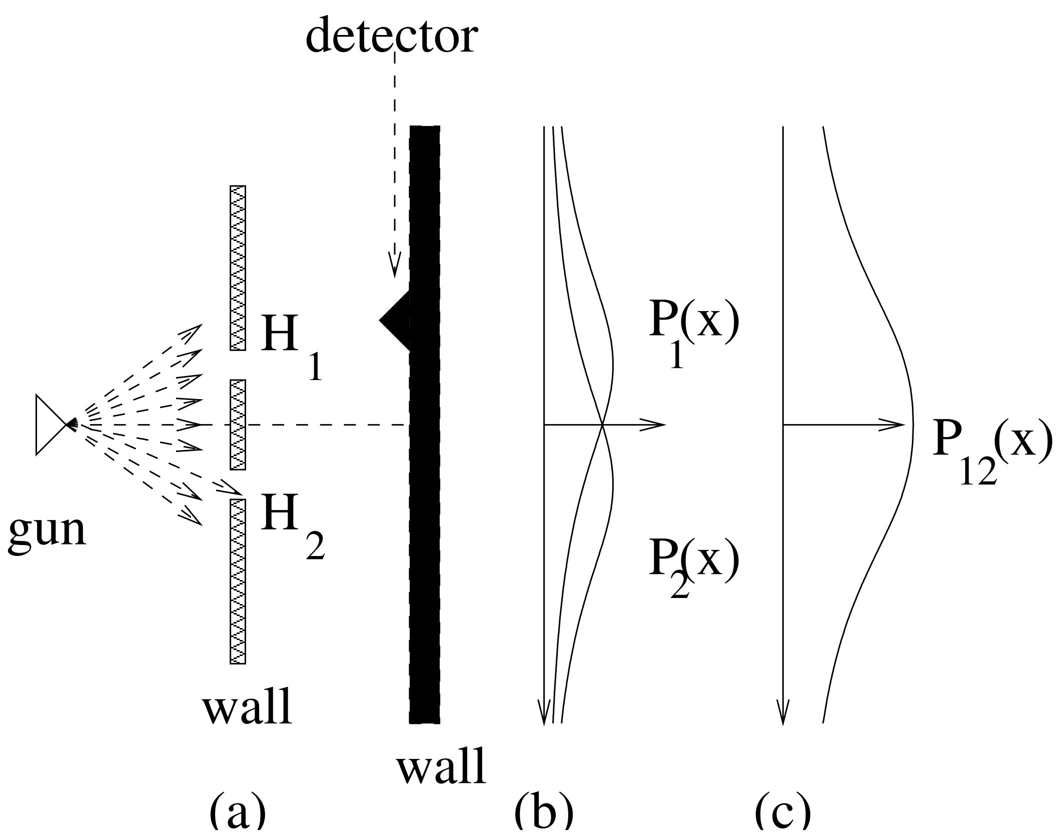


Figure 6: Experiment with bullets

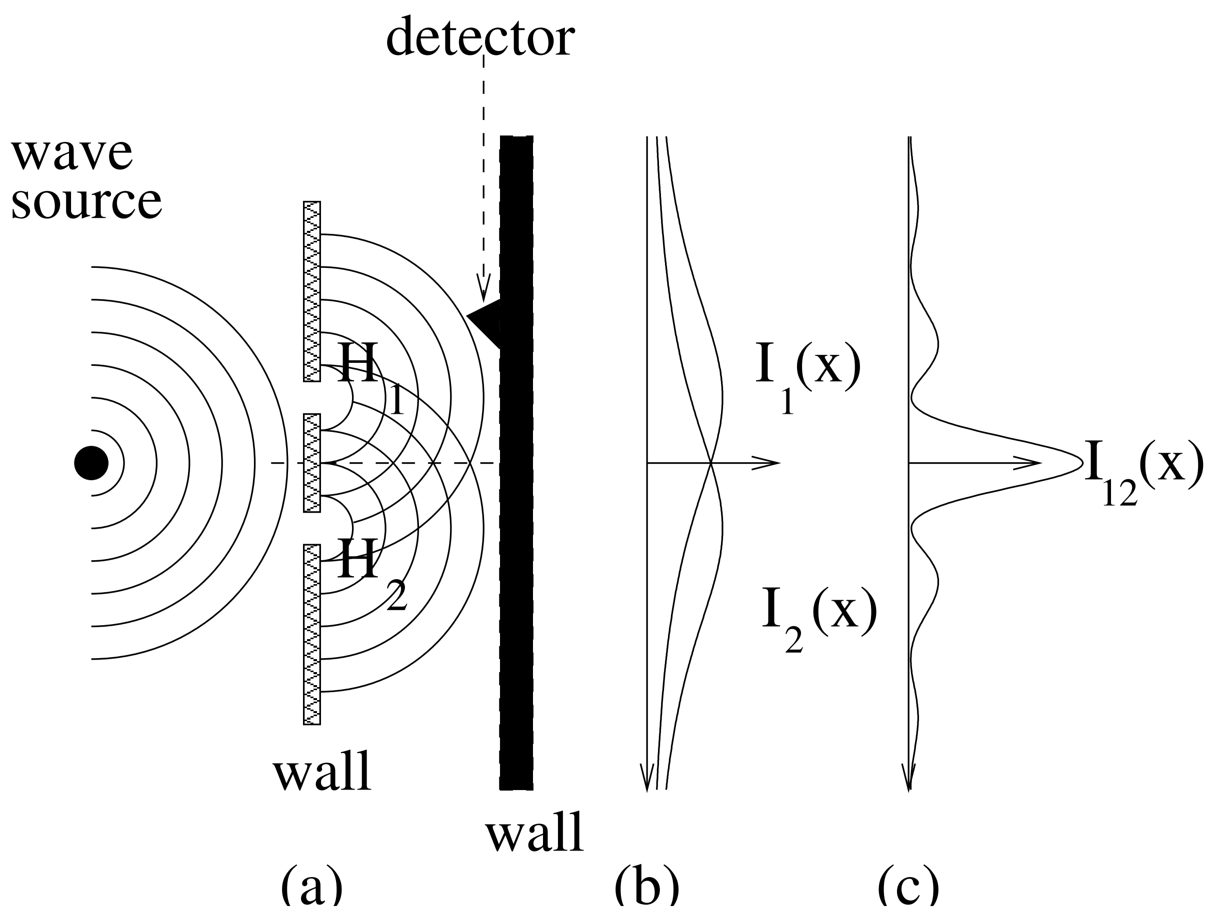


Figure 7: Experiments with waves

QUANTUM EXPERIMENTS

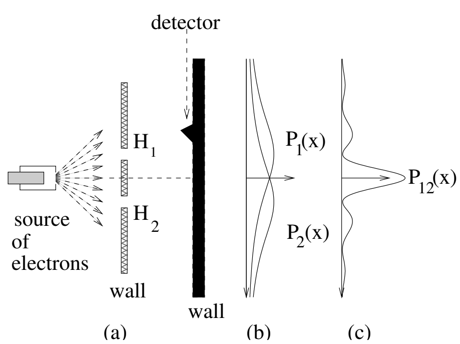


Figure 8: Two-slit experiment

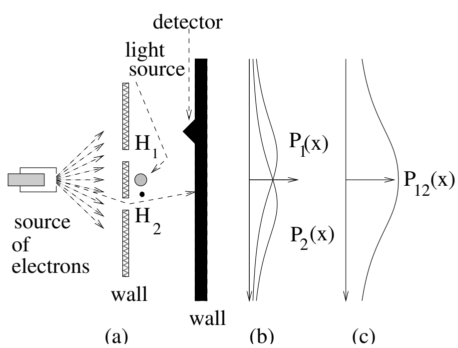


Figure 9: Two-slit experiment with an observation

QUANTUM EXPERIMENTS

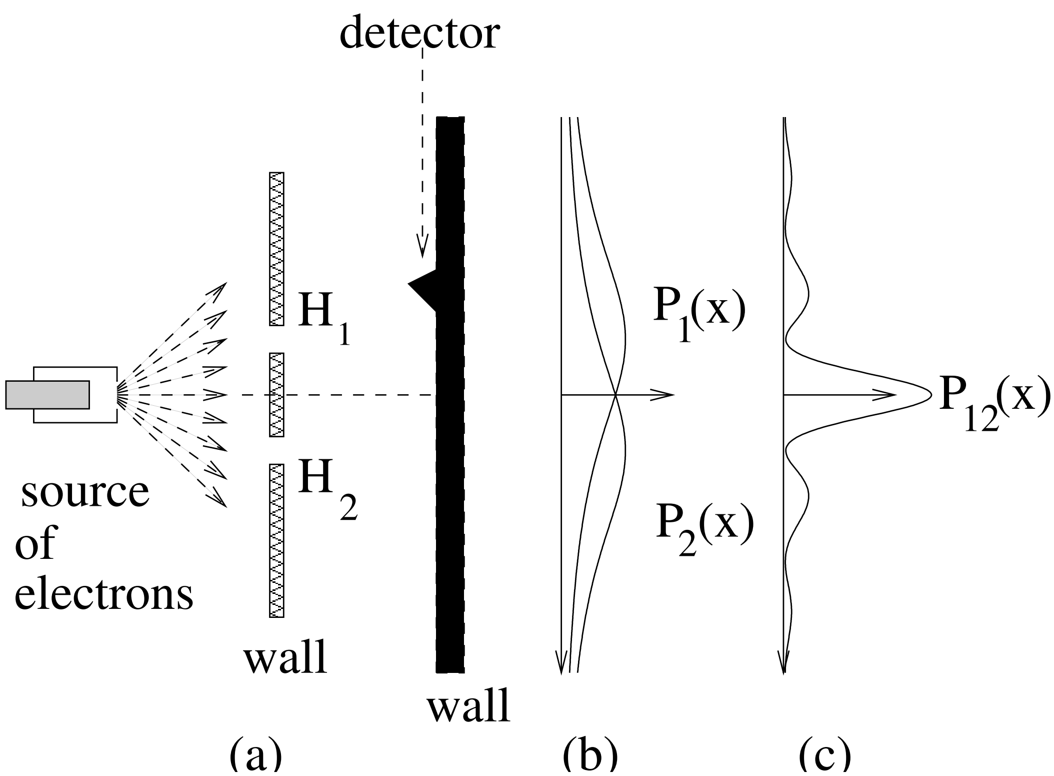


Figure 10: Two-slit experiment

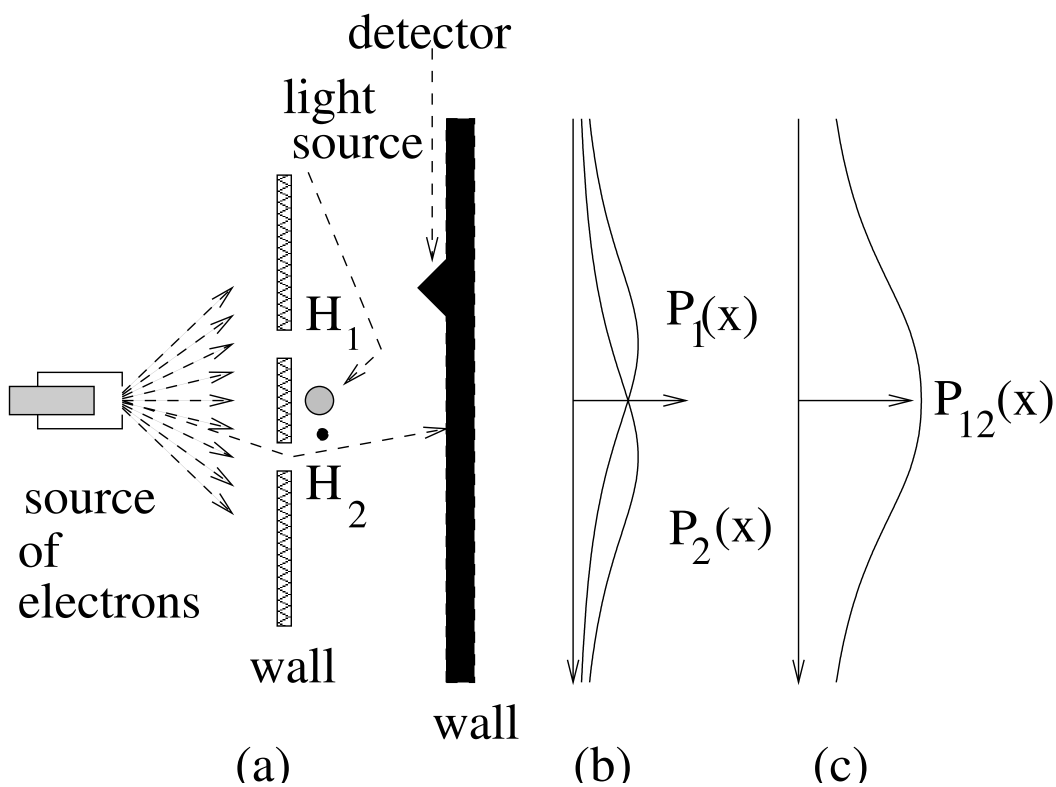


Figure 11: Two-slit experiment with an observation

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.

BOHR's WAVE-PARTICLE DUALITY PRINCIPLES

- Things we consider as waves correspond actually to particles and things we consider as particles have waves associated with them.
- The wave is associated with the position of a particle - the particle is more likely to be found in places where its wave is big.
- The distance between the peaks of the wave is related to the particle's speed; the smaller the distance, the faster particle moves.
- The wave's frequency is proportional to the particle's energy. (In fact, the particle's energy i s equal exactly to its frequency times Planck's constant.)

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

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

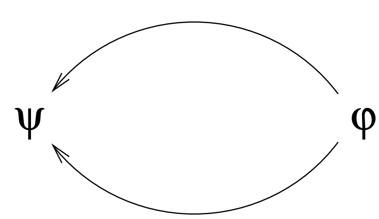
is the **probability** of the transfer.

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 sub-transfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from ϕ to ψ has two independent alternatives, with amplitudes α and β



then the resulting amplitude is the sum $\alpha + \beta$ of amplitudes of two sub-transfers.

QUANTUM SYSTEM = HILBERT SPACE

Hilbert space $\mathcal{H}_n$ is n-dimensional complex vector space with

scalar product

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

norm of vectors

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

and the metric

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

This allows us to introduce on $\mathcal{H}$ a 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 $f : H \to \mathbf{C}$ there exists a unique $\phi_f \in H$ such that $f(\psi) = \langle \phi_f | \psi \rangle$ for any $\psi \in H$.
Elements (vectors) of a Hilbert space $\mathcal{H}$ are usually called **pure states** of H.

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

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

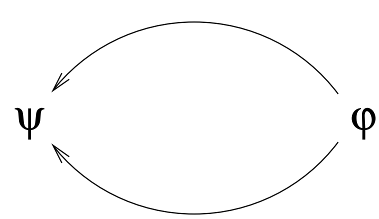
is the **probability** of the transfer.

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 sub-transfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If the transfer from ϕ to ψ has two independent alternatives, with amplitudes α and β



then the resulting amplitude is the sum $\alpha + \beta$ of amplitudes of two sub-transfers.

ORTHOGONALITY of PURE STATES

Two quantum states $|\phi\rangle$ and $|\psi\rangle$ are called orthogonal if their scalar product is zero, that is if

$$\langle\phi|\psi\rangle = 0.$$

Two pure quantum states are physically perfectly distinguishable only if they are orthogonal.

In every Hilbert space there are so-called orthogonal bases all states of which are mutually orthogonal.

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

Dirac 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

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

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

$\langle\psi|$ **— bra-vector – a row vector - the conjugate transpose of $|\psi\rangle$ – a linear functional on H such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$**

Example If $\phi = (\phi_1, \ldots, \phi_n)$ and $\psi = (\psi_1, \ldots, \psi_n)$, then

ket vector - $|\phi\rangle = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix}$ **and** $\langle\psi| = (\psi_1^*, \ldots, \psi_n^*)$ $-$ **bra-**

and

inner product - scalar product: $\langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i$

outer product: $|\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \ldots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \vdots & \phi_n\psi_n^* \end{pmatrix}$

The meaning of the out-product $|\phi\rangle\langle\psi|$ is that of the mapping that maps any state $|\gamma\rangle$ into the state

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

It is often said that physical counterparts of vectors of n-dimensional Hilbert spaces are n-level quantum systems.

QUBITS

A **qubit** - a two-level quantum system 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

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

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom — (b) a spin-$\frac{1}{2}$ particle

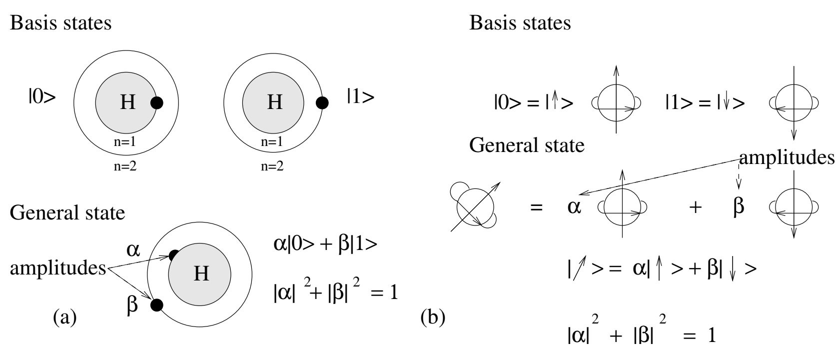


Figure 12: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

x

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

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

HILBERT SPACE H_2

STANDARD (COMPUTATIONAL) BASIS DUAL BASIS

$$|0\rangle, |1\rangle \qquad\qquad |0'\rangle, |1'\rangle$$

$$\begin{pmatrix}1\\0\end{pmatrix} \begin{pmatrix}0\\1\end{pmatrix} \qquad\qquad \begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix} \begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}$$

Hadamard matrix (Hadamard operator in the standard basis)

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

has properties

$$H|0\rangle = |0'\rangle \qquad\qquad H|0'\rangle = |0\rangle$$

$$H|1\rangle = |1'\rangle \qquad\qquad H|1'\rangle = |1\rangle$$

and transforms standard basis $\{|0\rangle, |1\rangle\}$ into dual (or Hadamard) basis $\{|0'\rangle = |+\rangle, |1'\rangle = |-\rangle\}$ and vice verse.

QUANTUM EVOLUTION/COMPUTATION

EVOLUTION
COMPUTATION

in in

QUANTUM SYSTEM
HILBERT SPACE

is described by

Schrödinger linear equation

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

where $H(t)$ is a Hermitian operator representing total energy of the system, from which it follows that $\psi(t) = e^{-\frac{i}{\hbar}H(t)}$ and therefore that an discretized evolution (computation) step of a quantum system is performed by a multiplication of the state vector by a **unitary operator**, i.e. a step of evolution is a multiplication by a **unitary matrix** A of a vector $|\psi\rangle$, i.e.

$$A|\psi\rangle$$

A matrix A is **unitary** if for A and its adjoin matrix $A^\dagger$ (with $A^\dagger_{ij} = (A_{ji})^*$) it holds:

$$A \cdot A^\dagger = A^\dagger \cdot A = I$$

ANOTHER VIEW of UNITARITY

A unitary mapping U is a linear mapping that preserves the inner product, that is

$$\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle.$$

HAMILTONIANS

The Schrödinger equation tells us how a quantum system evolves

subject to the Hamiltonian

However, in order to do quantum mechanics, one has to know how to pick up the Hamiltonian.

The principles that tell us how to do so are real bridge principles of quantum mechanics.

Each quantum system is actually uniquely determined by a Hamiltonian.

UNITARY MATRICES — EXAMPLES

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

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

Hadamard matrix $= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ $\quad \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix} =$

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

Pauli matrices play a very important role in quantum computing.

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.

A UNIVERSAL SET of QUANTUM GATES

The main task at quantum computation is to express solution of a given problem P as a unitary matrix U_P and then to construct a circuit C_{U_P} with elementary quantum gates from a universal se ts of quantum gates to realize U. That is

$$P \rightarrow U_P \rightarrow C_{U_P}.$$

A simple universal set of quantum gates consists of gates

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4}i} \end{pmatrix}$$

SOLVING SCHRÖDINGER EQUATION

For the Hamiltonian

$$H = \frac{\pi\hbar}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} = \frac{\pi\hbar}{2}V$$

the Schödinger equation

$$i\hbar\frac{\partial U(t)}{\partial t} = HU(t)$$

has the solution

$$U(t) = e^{-\frac{i}{\hbar}Ht} = \sum_{k=1}^{\infty}\frac{(-\frac{i\pi}{2})^k V^k t^k}{k!} = I + \frac{1}{2}\sum_{k=0}^{\infty}\frac{(-\pi i t)^k}{k!}V$$

and therefore for $t = 1$,

$$e^{-\frac{i\pi}{2}V} = I + \frac{1}{2}(e^{-i\pi} - 1)V = I - V = CNOT.$$

STRUCTURE of ATOMS - BASIC FACTS

- Atoms are typically a few billions of a metre across spheres held together by electricity.
- An atom has a compact nuclei (100 000 times smaller) consisting of (positively charged) protons and (without charge) neutrons;
- A nucleus is surrounded by a cloud of electrons whose masses are a couple of thousands times smaller that those of protons and neutrons;
- Electrons are negatively charged and there are so many neutrons as protons and therefore each atom as the whole is electrically neutral.
- Each electron has a wave associated with its position and velocity. The places where wave is big are places where electrons are likely to be found. The shorter the length of the wave, the faster electron is moving.
- The rate at which the wave wiggles up and down is proportional to electron's energy.
- Suppose we want to fit electron's wave around an atom's nuclei. The simplest wave that can fit around a nucleus is a sphere; the next simplest way has one peak, then two and so on. Each of these types of waves corresponds to an electron in a definite energy state. The more peaks has an electron's wave, more energy it has.

- When an electron jumps from a higher energy state to a lower energy state it emits a photon whose energy equals of energy difference of two states. Similarly, an atom can absorb a photon and jump from one energy level to a higher energy level. Any atoms refuses to absorb a photon whose energy is not exactly the difference of some energy levels.
- Emitting or absorbing a photon takes some time.
- Usually we take the ground state (corresponding to lowest energy level) as representing $|0\rangle$ and the next exciting state as representing the state $|1\rangle$.
- An application of a laser pulse takes an atom from state $|0\rangle$ to $|1\rangle$ and vice verse.

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 mutually 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 de-composability 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 $\phi_i \in W_i, 1 \leq i \leq n$.