I. Why Quantum Mechanics?

Quantum Mechanics (QM) dramatically changed our understanding of this world. As a result, all physics theories are partitioned into two big families: **Classical Theories** and **Quantum Theories**.

QM is a foundation of all modern theories of elementary particles and their interactions, Fig. 1.

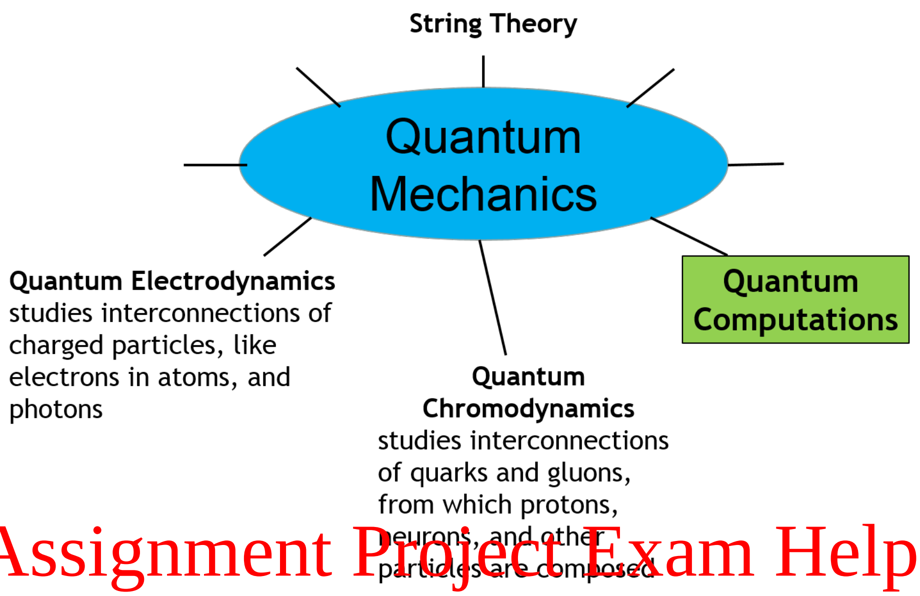

Fig. 1: QM is a foundation of all modern theories of elementary particles

There are no alternatives to QM. No observations have been made that would contradict to QM. QM predictions are confirmed with super accuracy, up to 10^{-8}.

At the end of the 19-th century we had two fundamental theories – Newtonian Mechanics and Maxwell's Electrodynamics. However these theories led to multiple contradictions. Below we consider two such contradictions.

A. *The Atomic Stability Problem*

The Rutherford experiments showed that atoms consist of protons $(+)$ and electrons $(-)$. The popular model of atom is the planetary model in which electrons orbit around massive nucleus, Fig. 2.

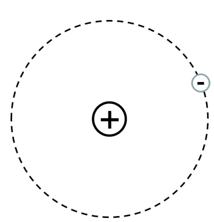

Fig. 2: Planetary model of atom

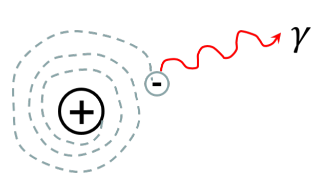

Fig. 3: Atomic stability problem

However, according to Maxwell's Electrodynamics a charged particle moving along an orbit must emit electromagnetic waves. These waves carry energy, which should be taken from the electron kinetic energy. Hence within a tiny time interval electrons should drop on nucleus, Fig. 3. This does not happen in reality.

B. The Atomic Spectra Problem

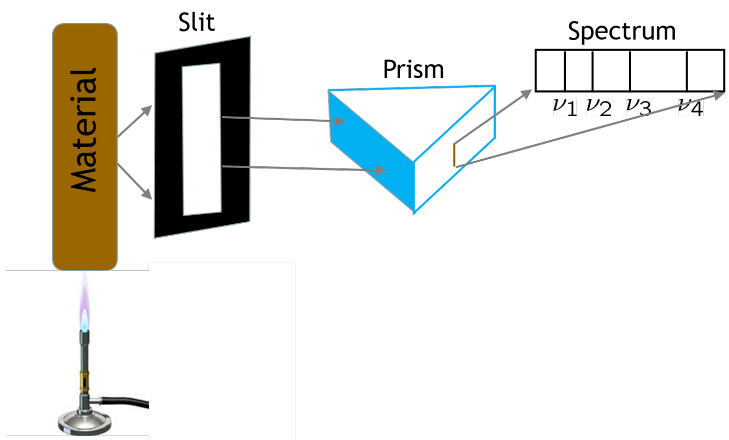

Fig. 4: Spectrum of atom

Let us conduct the experiment shown in Fig. 4. An atom emits and absorbs electromagnetic waves of particular frequencies $\nu_1, \nu_2, \ldots, \nu_n$, but not of the frequency say $\nu_i < \nu < \nu_{i+1}$, Fig. 5.

Fig. 5: Atom emits and absorbs electromagnetic waves of particular frequencies

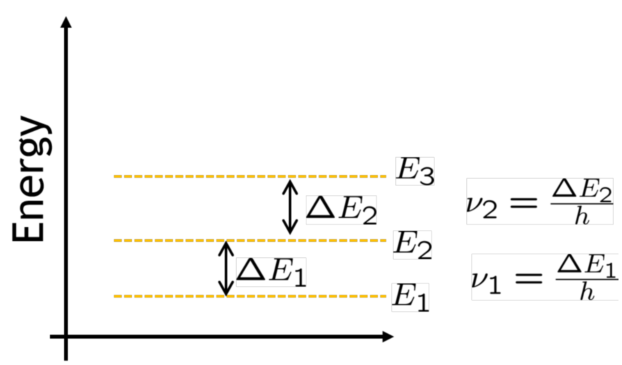

Fig. 6: Spectrum of Atom

The atomic spectrum is unique. This allows us, in particular, to figure out the chemical compositions of stars by observing and analyzing their light. Each frequency from the spectrum corresponds to a particular emission energy, Fig.6. The classical theories did not give an explanation why we observe these levels, and did not allow one to figure out the values.

II. Counterintuitive Quantum Mechanical Experiments

Below we consider several QM experiments that look very counterintuitive from the classical reasoning point of view.

A. *Interference of Qubit (Elemetray Particle) with Itself*

1) Double-Slit Experiment: Let us assume that we have a source that emits single electrons toward a wall with a double-slit. Most of the electors are absorbed by the wall, but some will travel through the slits. If we use classical reasoning, then we expect to see on the screen behind the wall two strips of marks roughly the same shape as the slits, as it is shown on Fig. 7.

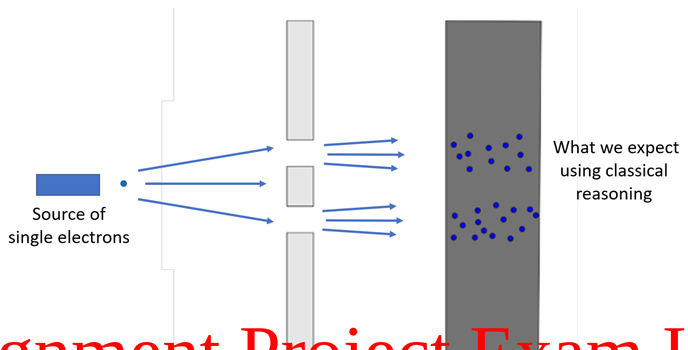

Fig. 7: Double Slit Experiment: Classical Reasoning

However, if we conduct a real experiments, we will see multiple stripes, similar to what is shown in Fig. 8 and Fig. 9.

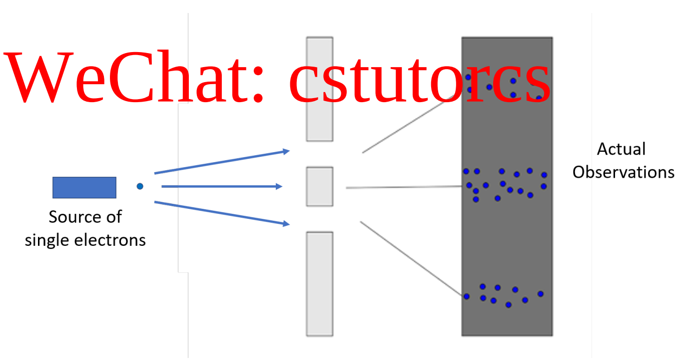

Fig. 8: Double Slit Experiment: QM Prediction

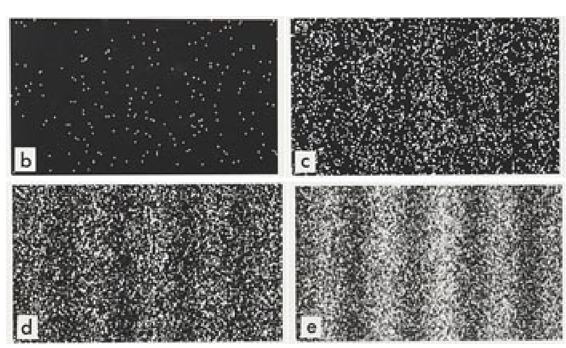

Fig. 9: Real Experiment Observations. Going from (b) to (e) corresponds to increase in the number of emitted electrons in experiment. We see that the more electrons are emitted, the more pronounced are the stripes

If instead of single electors we use electro-magnetic waves, we will see similar interference stripes, Fig. 10. The reason for these stripes is the well known effect of interference of electromagnetic waves. In our experiment we have two waves at the outputs of the slits. These waves interfere with each other (constructively or destructively), in other words they sum up together, which results in the stripes left on the screen.

This experiment shows that a single elector (and other elementary particles) behaves like it goes through both slits simultaneously and further interferes with itself!

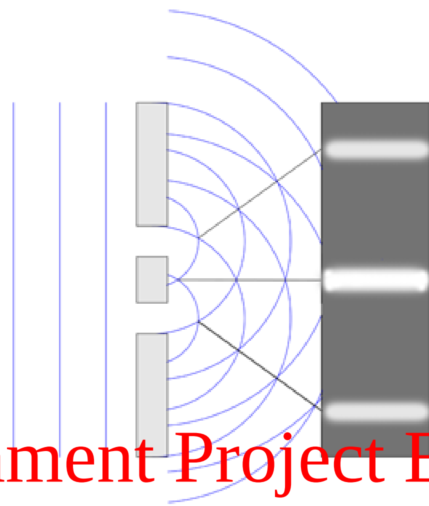

Fig. 10: Double Slit Experiment 1

B. *Photon in Superposition States*

Let us have a source of single photons and a semi-transparent mirror. This mirror reflects a photon with probability $1/2$ and allows a photon to go through also with probability $1/2$, as it shown in Fig. 11.

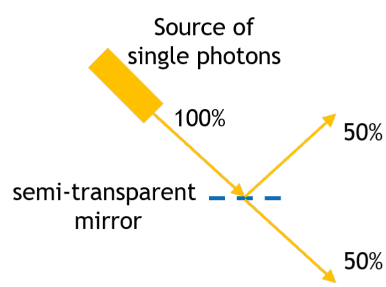

Fig. 11: Interference of Photon 1

Let us add to the experiment two usual mirrors and one more semi-transparent mirror as it shown in Fig. 12. Thinking classically, we would expect that after interaction with the second semi-transparent mirror a photon will be at the upper or bottom outputs with probabilities $1/2$ and $1/2$, and we will observe 50% and 50% of photons at both outputs.

However, real life experiments demonstrate an absolutely different result shown in Fig. 13. All 100% of photons appear at the bottom output.

This is a very surprising result. QM explains it in the following way. In this experiment each photon can be in one of the two orthogonal states: $|\searrow\rangle$ or $|\nearrow\rangle$. Numerically these states can be represented by the following two orthogonal vectors:

$$|\searrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |\nearrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

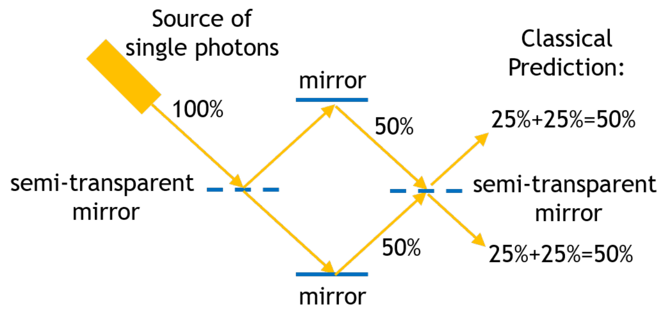

Fig. 12: Interference of Photon 2

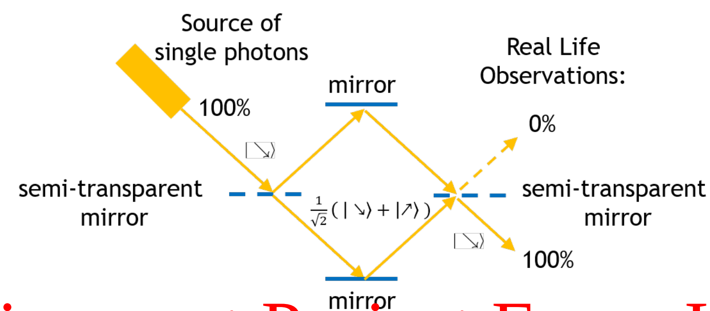

Fig. 13: Interference of Photon 3

The semi-transparent mirrors are modeled by the unitary operator (matrix):

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

The quantum mechanical time evolution of a photon can be described as follows.

1) In the very beginning each photon is in the state $|\searrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
2) After interaction with the first semi-transparent mirror its state becomes

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = U \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Note that this state is a superposition of the states $|\nearrow\rangle$ and $|\searrow\rangle$. In classical mechanics this is not possible of course. Somebody can say that it looks like that the photon splits out along the two routes. This, however, is a wrong interpretation, since photon is an elementary particle and it cannot split.
3) The two mirrors in the middle do not change the superposition state (we omit details of this).
4) After interaction with the second semi-transparent mirror the photon state becomes

$$|\searrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = U \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Let us install now a single-photon detector in one of the photon routes, as it is shown in Fig. 14. If the detector detects a photon, the photon does not go any further since it is absorbed by the detector. Thus, only 50% of all the photons, those that went along the upper route, reach the second semi-transparent mirror. Taking into account our previous observation that we have 0% of photons at the upper output and 100% of photons at the lower output, it is naturally to assume that now we will observe 50% of all the photons at the lower output. However, in real life we observe 25% of photons at each output. This

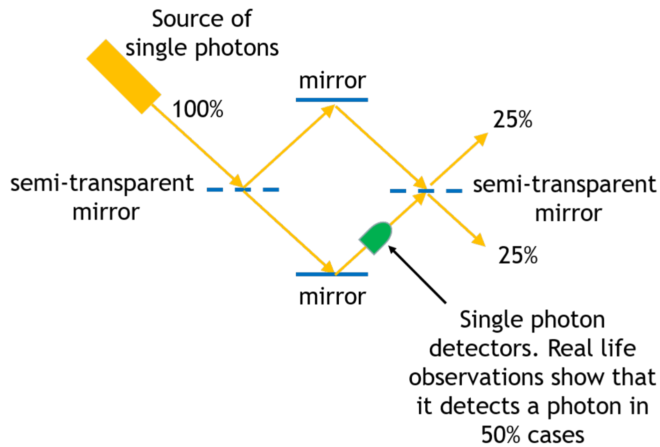

Fig. 14: Interference of Photon 4

happens because the presence of the detector leads to a collapse of the superposition. Later this will be formulated as one of the QM postulates - *revealing any information about the state of an elementary particle results in that its state collapses to one of the orthogonal states*. We will study this, and other, QM postulates in full details soon.

How to explain all these unexpected observations? Our classical intuition cannot help us here. The only thing we can do is to develop a formal mathematical theory that would allow us to predict results of experiments.

III. Elitzur–Vaidman Bomb Tester

Let us assume that we have a set of fake and real bombs. A real bomb explodes if even a single photon hits it, Fig. 15. Our goal is to find real bombs without exploding them of course. This looks like "mission impossible".

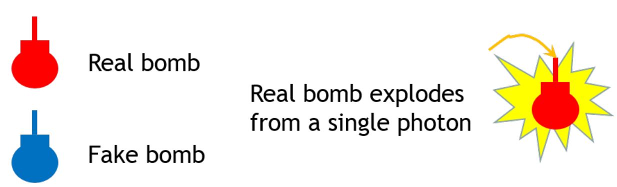

Fig. 15: Elitzur–Vaidman Bomb Tester 1

However the experiment considered in the previous section will allow us to do this. We assume that the bottom mirror can be used as detonator (mirror detonator), as it shown in Fig. 16 and Fig. 17. As soon as a photon hits that mirror detonator a real bomb explodes.

Let us assume that we attached a fake bomb to the mirror detector, Fig. 16. Since the bomb is fake and it will not explode in any case, we will not get any information about whether photon goes along the upper route or the bottom route. Thus, this case is equivalent to the case shown in Fig. 13 and all photons will be in the superposition and eventually observed at the lower output.

If we attach a real bomb to the mirror detector, then this scenario becomes similar to the setting in Fig. 14, since if bomb explodes this reveals us that the photon went through the bottom route. Thus, the photon will be not in the superposition state. Instead, it will go through either upper route or bottom route with probabilities $1/2$ and $1/2$. If the photon goes along the bottom route the bomb explodes. However, if the photon goes along the upper route then the bomb does not explode and the photon will be observed at upper or bottom outputs with probabilities $1/2$ and $1/2$. In the case the photon goes along the bottom route, the bomb explodes. In the case photon goes along the upper route, the bomb does not explodes

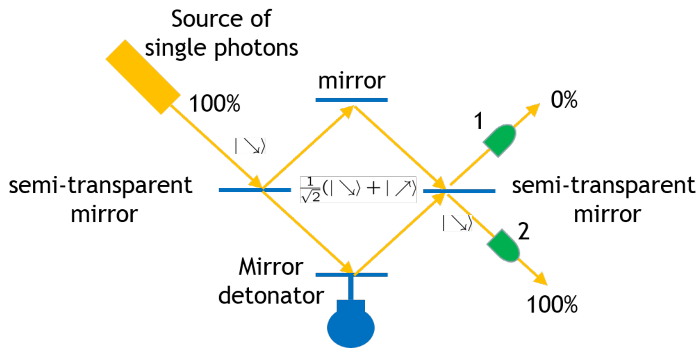

Fig. 16: Elitzur–Vaidman Bomb Tester 2

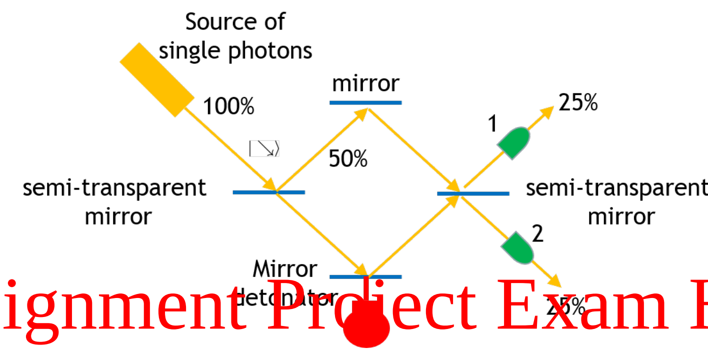

Fig. 17: Elitzur–Vaidman Bomb Tester 3

and after interaction with the second semi-transparent mirror the photon will be observed at the upper and lower outputs with probabilities $1/2$ and $1/2$. If the photon is observed at the upper output, then we know for sure that the bomb is real, and we did not exploded it!

Thus way we can identify $1/4$ of real bombs without exploding them. Amazing, isn't it?

IV. Quantum Entanglement or Mystery of Quantum Cakes

Let us assume that we have a kitchen with opposite doors and two conveyor belts, Fig. 18. Pairs of ovens come on the belts from the opposite directions to the kitchen. Lucy (left) can either open her oven in the middle of the journey and check whether batter has Risen or Not Risen (measurement 1), or can taste the cake when its baked in the kitchen and decided whether it is Good or Bad (measurement 2). Ricardo (right) can do the same. It is not allowed to make both measurements for the same cake (one possible reason for this is that if the oven is open in the middle of its journey, then the required temperature regime would be destroyed).

Lucy and Ricardo conduct measurements randomly and independently and observe that

Fig. 18: Fabric of Quantum Cakes

1) Luce and Ricardo both make measurement 1: in 9% cases they saw that batter Rose for both of then;
2) Lucy makes measurement 1 and Ricardo makes measurement 2: if Lucy observes Risen batter, then Ricardo observes Good taste;
3) Ricardo makes measurement 1 and Lucy makes measurement 2: if Ricardo observes Risen batter, then Lucy observes Good taste.

The question is what will they get when both make measurement 2? Using classical reasoning, we should conclude that at least in 9% cases both cakes will taste Good. However, using quantum entanglement (we will study it in the course), cakes can be prepared so that Lucy and Ricardo will never get both cakes being Good.

V. Quantum Computing

- 1980, Richard Feynman said
  - use q. computer to simulate physical systems (interactions of atoms),
  - q. computers will beat classical computers.
- 1995, Peter Shor proposed
  - q. factoring algorithm. Let $n = p_1 p_2 \dots p_t$, where p_j are prime factors. Then q. computer can find the primes p_j in polynomial time (exponential speed up over classical computers),
  - showed that this leads to breaking RSA cryptosystem, which is used very actively by US government, banks, and so on.

- 1995, some researchers say
  - q. states are fragile,
  - non cloning theorem prevents us from duplicating (cloning) q. states,
  - therefore even the classical repetition code (the simplest classical error correcting code that encodes 0 into $(0,0,0,0,0)$ and 1 into $(1,1,1,1,1)$) is not applicable in q. case, and, therefore, we will never be able to build a quantum computer.

- 1995, Peter Shor
  - showed that q. error correction is possible, and proposed the first q. code that encodes 1 qubit into 9 qubits and corrects any single error.
- 1996, Love Grover
  - proposed q. search algorithm. Let

$$f(i) = \begin{cases} 0, & i \neq i^*, \\ 1, & i = i^*, \end{cases} \quad , i = 0, \dots, N-1.$$

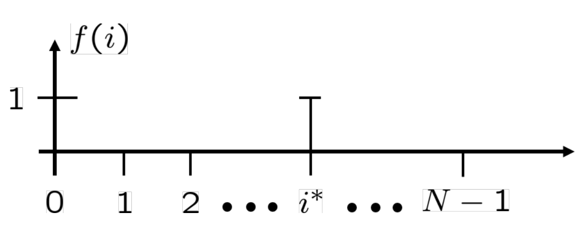

Fig. 19: Fast Quantum Search

The problem is to find i^*. Classical computer needs to evaluate $f(i)$ $N-1$ times. Q. computer needs to evaluate $f(i)$ only $\sqrt{N}$ times.

- Killing application of quantum computers
  - simulation of physical systems. To simulate a system of 75 atoms we have to operate with vectors in $\mathbb{C}^{2^{75}}$, which is impossible even for classical supercomputer. Q. computer (assuming that all its qubits and gates are error free) needs to operate only with 75 qubits in this task.

- Companies that actively work on q. computing: Google, IBM, Microsoft, D-Wave, Intel, BBN Technologies, Rigetti, NIST, IonQ, MiTRE, and many others.

VI. Types of Quantum Computing

- **Universal Fault-Tolerant Quantum Computer**
  - This is the subject of this course.
  - Such computer would allow one to run useful algorithms with large and very large speed-ups over any classical counterpart, including classical supercomputers.
  - This type of computers need quantum error correction.
- **Approximate Noisy Intermediate Scale Quantum (NISQ Computers)**
  - We hope to these devices will be available soon.
  - They are not fault tolerant and therefore operate over noisy qubits.
  - They still can be useful for a number of applications, like quantum chemistry, numerical methods, AI, and others.
- **Analog or Quantum Annealing Devices (DWave)**
  - System that use quantum effects to solve and/or emulate certain specific problems.
  - They have limited programmability, and at this moment it is not clear whether they can provide a speed-up over conventional computers.
  - They already operate with a large (2000 and more) qubits.

VII. Promisin Quantum Research/Development Directions

- **Quantum Computers**
  - Quantum computers promise to be drastically faster than classical computers.
  - According to Moore's law the number of transistors on a microchip doubles about every two years. So, the size of transistor decreases exponentially fast ($1/2^n$, n is the number of years). If we continue in this way, then by 2030 transistors will have atomic size, and will start behaving according to QM laws. Thus, we must study quantum computations and quantum computers already now.

- **Quantum Internet**
  - Linking multiple quantum processors through a quantum network, in order to get a more powerful quantum device.
  - Multi-party secure communication.
  - Building an array of interferometric telescopes to boost the angular resolution of astronomical images.
  - Super precise network clocks synchronization.
  - People already work on developing quantum internet protocols. These protocols are in some sense similar, but still quite different from classical protocols, like TPC, since they deal with communication of qubits, not bits.
- **Quantum Simulations in material science**
  - Such simulation is a very tough problems, since we must model iterations of very large number of entangled atoms.
  - This could be very important for designing new materials, for example materials with high temperature superconductivity, new drugs, and similar things.
- **Quantum Cryptography**
  - Commercial equipment for Quantum Key Distribution (QKD) is already available.
  - In 2017 physicists from the University of Science and Technology of China organized QKD via satellite Micius between Beijing, China, and Vienna, Austria. In this experiment Images and videos were transmitted securely between Vienna and Beijing.

- There are still many open research and development problems.

- **Quantum Telemetry**
  - We replace an atom in a crystal lattice with another atom. The state of this new atom is very sensitive to magnetic and electric fields around it. We can control this new atom and read its state.
  - This would allow us to judge what is going in some very small objects. For example, there is a hope that this will allow us to understand how a biological cell works, whether it is healthy or not and so on.
  - Another promising idea is to build an atomic chronometer. Such a chronometer would be very useful for very precise geo-positioning.

VIII. Mathematical Foundations of QM

Colorful movies and presentations, sophisticated comparisons and analogues from our classical world, do not allow us to understand QM and predict results of experiments with elementary particles. The only productive way is developing a formal (mathematical) theory of QM.

There are two important parts of QM- finite dimensional analysis and infinitely dimensional analysis. Finite dimensional case is significantly simpler. Good news that for Quantum Computations (QC) we need, in most algorithms, only this simple case. So, in this course we will mostly focus on the finite dimensional formalism, and will only briefly consider the infinitely dimensional case.

A. Basic Notations and Notions of Linear Algebra

QM operates with matrices and vectors over complex field $\mathbb{C}$ according to the standard rules of linear algebra.

Let $i \in \mathbb{C}$ be the imaginary one, i.e., $i^2 = -1$. Summation and multiplication of complex numbers defined by

$$(a+ib)+(c+id) = (a+c)+i(b+d), \; (a+ib)(c+id) = ac - bd + i(ad+bc), \;\; a,b,c,d \in \mathbb{R}.$$

The *conjugation* and the *absolute value* of a complex number $a+ib$ are defined by

$$(a+ib)^\dagger = a - ib, \;\; |a+ib| = \sqrt{a^2+b^2}.$$

Multiplication of matrices, and multiplication of matrix by vector are conducted according to the standard rule "row by column", e.g.,

$$\begin{pmatrix} 2i & 3 \\ -4i & 5i \end{pmatrix} \begin{pmatrix} i \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 4+i10 \end{pmatrix}.$$

Hermitian conjugation of a matrix is denoted by $\dagger$ and is obtained by matrix *transposition*, which is denoted by T, and conjugation of all its entries, e.g.,

$$\begin{pmatrix} 2i & 3 \\ -4i & 5i \end{pmatrix}^\dagger = \begin{pmatrix} -2i & 4i \\ 3 & -5i \end{pmatrix}.$$

The norm of vector $\mathbf{v} = (v_1, \ldots, v_n)^T$ is defined by

$$||\mathbf{v}||^2 = |v_1|^2 + \ldots + |v_n|^2.$$

For example,

$$||(i,2)^T||^2 = 1 + 4 = 5.$$

The *standard basis* of $\mathbb{C}^N$ is the set of vectors $\mathbf{v}_0, \ldots, \mathbf{v}_{N-1}$, where

$$\mathbf{v}_j = (0, \ldots, 0, \underbrace{1}_{j\text{-th position}}, 0, \ldots, 0)^T, \;\; j = 0, \ldots, N-1.$$

For example, in the case of $\mathbb{C}^4$ the standard basis is

$$\mathbf{v}_0 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad \mathbf{v}_1 = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad \mathbf{v}_2 = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad \mathbf{v}_3 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{1}$$

Any vector $\mathbf{v} \in \mathbb{C}^N$ can be represented as a linear combination (superposition) of vectors $\mathbf{v}_0, \ldots, \mathbf{v}_{N-1}$

$$\mathbf{v} = \alpha_0 \mathbf{v}_0 + \ldots + \alpha_{N-1}\mathbf{v}_{N-1}, \;\; \alpha_j \in \mathbb{C}.$$

The *inner product* of vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^N$ is defined by

$$\mathbf{v}^\dagger \mathbf{w} = v_0^\dagger w_0 + \ldots + v_{N-1}^\dagger w_{N-1} \in \mathbb{C}.$$

Note that the standard basis is an *orthonormal* basis (basis of mutually orthogonal vectors of norm one) since

$$||\mathbf{v}_j|| = 1 \text{ and } \mathbf{v}_j^\dagger \mathbf{v}_k = 0 \text{ for } j \neq k.$$

The identity matrix I_N is the diagonal matrix whose all diagonal entries are 1s, e.g.,

$$I_3 = \begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}.$$

The *inverse* of a matrix $A \in \mathbb{C}^{N\times N}$ is the matrix A^{-1} such that $A^{-1}A = AA^{-1} = I_N$. For example

$$A = \begin{pmatrix}2i & 4\\-4i & 8i\end{pmatrix}, \; A^{-1} = \begin{pmatrix}\frac{1}{4}(1-i) & \frac{1}{8}(1+i)\\ \frac{1}{8}(1-i) & \frac{1}{16}(1-i)\end{pmatrix}, \; A^{-1}A = AA^{-1} = I_2.$$

A matrix U is called *unitary* if $U^{-1} = U^\dagger$. For example

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\1 & -i\end{pmatrix}, \; U^\dagger = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\-i & i\end{pmatrix}, \; UU^\dagger = U^\dagger U = I_2.$$

B. *Dirac Notations*

Let $\mathbf{v}_0, \ldots, \mathbf{v}_{2^n-1}$ be the standard basis of $\mathbb{C}^{2^n}$. Then

Linear Algebra		Dirac Notation
$\mathbf{v}_j$	$\Leftrightarrow$	$\mid$ binary representation of $j\rangle$ or $\mid j>$

For example, $\mathbf{v}_5 \in \mathbb{C}^{2^3}$ corresponds to $|101\rangle$ or $|5\rangle$. One more example - for $\mathbb{C}^{2^2}$ we have

Linear Algebra		Dirac Notation
$\mathbf{v}_0$	$\Leftrightarrow$	$\mid 00\rangle$ or $\mid 0>$
$\mathbf{v}_1$	$\Leftrightarrow$	$\mid 01\rangle$ or $\mid 1>$
$\mathbf{v}_2$	$\Leftrightarrow$	$\mid 10\rangle$ or $\mid 2>$
$\mathbf{v}_3$	$\Leftrightarrow$	$\mid 11\rangle$ or $\mid 3>$.

The Dirac notation for the Hermitian conjugated vector is

Linear Algebra	vs	Dirac Notation
$\mathbf{v}_j^\dagger$	$\Leftrightarrow$	$\langle$ binary representation of $j\mid$ or $\langle j\mid$

Thus, $\mathbf{v}_5^\dagger$ corresponds to $\langle 101|$ or $\langle 5|$.

Using these notations we can replace all linear algebra notations with Dirac notations. For example, let $A \in \mathbb{C}^{2^n \times 2^2}$ be a complex matrix. Then

Linear Algebra	vs	Dirac Notation
$A\mathbf{v}_3$	$\Leftrightarrow$	$A\|11\rangle \in \mathbb{C}^{2^2}$
$\mathbf{v}_1^\dagger A\mathbf{v}_3$	$\Leftrightarrow$	$\langle 01\|A\|11\rangle \in \mathbb{C}$
$\mathbf{v}_1\mathbf{v}_3^\dagger$	$\Leftrightarrow$	$\|01\rangle\langle 11\| \in \mathbb{C}^{2^2 \times 2^2}$

Another example of using Dirac notation. Let

$$\mathbf{v} = 0.1\mathbf{v}_1 + 0.2\mathbf{v}_3 = 0.1|01\rangle + 0.2|11\rangle, \ \ \mathbf{w} = 0.3\mathbf{v}_1 + 0.5\mathbf{v}_2 = 0.3|01\rangle + 0.5|10\rangle.$$

Then

$$\begin{aligned} \mathbf{v}^\dagger \mathbf{w} &= (0.1\langle 01| + 0.2\langle 11|)(0.3|01\rangle + 0.5|10\rangle) \\ &= 0.03\langle 01|01\rangle + 0.05\langle 01|10\rangle + 0.06\langle 11|01\rangle + 0.1\langle 11|10\rangle = 0.03. \end{aligned}$$

Note that the product $|.\rangle\langle .|$ gives in a matrix, e.g.,

$$|01\rangle\langle 11| = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Sometimes it is useful to switch from Dirac Notation back to linear algebra notations. For example,

$$\begin{aligned} &\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \\ =&\alpha \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \delta \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}. \end{aligned}$$