Physics – Uspekhi **42** (5) 435 – 452 (1999)

REVIEWS OF TOPICAL PROBLEMS PACS number: **03.67.–a**

Quantum information

S Ya Kilin

Contents

Abstract. A new research direction known as quantum information is a multidisciplinary subject which involves quantum mechanics, optics, information theory, programming, discrete mathematics, laser physics and spectroscopy, and depends heavily on contributions from such areas as quantum computing, quantum teleportation and quantum cryptography, decoherence studies, and single-molecule and impurity spectroscopy. Some new results achieved in this rapidly growing field are discussed.

1. Introduction

Due to the rapid development of quantum optics at the end of the twentieth century, all of us, not only specialists in quantum physics but also people working far from this field, have to realize anew the basic statements of quantum theory. Indeed, quite abstract basic ideas of quantum physics, which recently seemed to deserve the attention of only a few specialists, are now important for almost everyone, because of their new applications in technology and, first of all, in optical interactions. Quantum computers, quantum teleportation and cryptography, observation and monitoring of single atoms, ions, molecules, including biological molecules — all these belong to the quantum world. This world is very difficult to explain in terms of our common classical world of macroscopic physics. For its description, it requires an adequate language of quantum mechanics and quantum field theory.

Quantum mechanics, created in the twenties by Niels Bohr (1885 – 1962), Erwin Schrödinger (1887 – 1961), Werner Heisenberg (1901 – 1976), and others, provided physicists with the recipes for calculating the energy states of atoms and molecules and the matrix elements of transitions between these states. However, in addition to this part, which immediately found applications in practical physics, quantum mechanics contained the 'ideological', philosophical part, which stayed almost 'unemployed' until recent years. It is this part of quantum mechanics that accounts for the odd nature of the quantum world. In the most complete and clear form, sometimes with deliberately paradoxical statements, this part of the quantum theory was presented by Erwin Schrödinger in his famous paper of 1935 [1], which he classified as 'a paper or a general confession' (''Referat oder Generalbeichte''). Using modern terminology, it deals with one of the problems of quantum information. The problem is: what information about the states of quantum objects can we get and what happens with the quantum objects while we are getting this information? More than half of a century passed before the basic principles formulated by Schrödinger became necessary for understanding experiments with practical applications.

In the present paper, we discuss several experiments of this kind. These are, first of all, experiments on quantum teleportation, quantum cryptography, and, finally, quantum computers, which are expected to be extremely beneficial but very difficult to construct. A certain part of the paper is devoted to single material particles in quantum optics and the methods of their detection. These objects can serve as the elements of quantum computers. In the conclusion, we consider the problem of decoherence and the possible ways of solving it, which is crucial for quantum computation. But

S Ya Kilin B I Stepanov Institute of Physics,
National Academy of Sciences of Belarus,
prosp. Frantsiska Scariny 70, 220602 Minsk, Belarus
Tel. (375-17) 284 26 13. Fax (375-17) 284 08 79
E-mail: kilin@ifanbel.bas-net.by

Received 18 June 1998
Uspekhi Fizicheskikh Nauk **169** (5) 507 – 527 (1999)
Translated by M V Chekhova; edited by L V Semenova

let us first discuss the language of quantum optics and the statements of quantum theory that are necessary for all further consideration.

2. Schrödinger and his famous paper of 1935

November 29, 1935. The journal *Die Naturwissenschaften* publishes the paper by E Schrödinger "Modern state of quantum mechanics" [1]. The paper was written during Schrödinger's compelled stay in Oxford (Fig. 1), after his winning, together with P Dirac, the Nobel prize in physics in 1933. As Schrödinger mentioned, his work originated from the discussion started on May 15, 1935 by Albert Einstein, Boris Podolsky, and Nathan Rosen in their paper "Can the Quantum Mechanical Description of Reality be Complete?" [2] and continued by Niels Bohr in his paper with the same title [3].

Figure 1. Erwin Schrödinger was born in Vienna. There he studied, first in a gymnasium, then in the university until graduation in 1910. Schrödinger started working in theoretical physics and soon became a professor in Breslau (now Wroclaw) and then in Zurich, where Einstein had worked earlier. In Zurich, Schrödinger published works that lead him to formulating the basic equation of non-relativistic quantum mechanics, the Schrödinger wave equation. For the development of quantum mechanics, Schrödinger together with Dirac was awarded the Nobel prize in 1933. In 1927, Schrödinger was invited to the chair of theoretical physics in Berlin, previously headed by Planck. When Hitler attained power, Schrödinger left fascist Germany and accepted an invitation to Oxford. In 1936, he returned to Austria for a short time and headed a chair in Graz, but after the Anschluss he had to leave his country again. This time Schrödinger moved to Ireland, to the Institute of Fundamental Research in Dublin. In 1947, he finally returned to his homeland. But his health was already failing, and after a long disease he died in Vienna. [The photograph and biographical note are taken from the anthology *Zhizn' Nauki* (Science life) (Ed. S P Kapitsa) (M.: Nauka, 1973).]

In spite of the abstract and complicated style of Schrödinger's paper [1], its importance was soon realized by Russian scientists, and it was immediately translated into Russian and published in 1936 in *Uspekhi Khimii* [1]. For comparison, the English translation appeared only in 1980 [1].

In his paper, Schrödinger analyses difficulties in the quantum mechanical description of measurement procedures and formulates four basic principles. According to these principles, the states of quantum objects have the following properties:

1. *Superposition*. A quantum state is described by a linear superposition of the basic states.

2. *Interference*. The result of measurement depends on the relative phases of the amplitudes in this superposition.

3. *Entanglement*. Complete information about the state of the whole system does not imply complete information about its parts.

4. *Nonclonability and uncertainty*. An unknown quantum state can be neither cloned nor observed without being disturbed.

Let us briefly comment on each of these statements. But first let us note that until recently, the third and the fourth principles were almost unknown to the majority of physicists and were discussed only in connection with the Einstein – Podolsky – Rosen (EPR) paradox and Bell's inequalities.

2.1 Superposition and the Schrödinger cat paradox

In contrast to a classical object, a quantum object has statistical origin. However, the probability nature of a quantum object cannot be understood as a classical uncertainty connected, for instance, with the incomplete knowledge about the object. For the description of a quantum object, the concept of a state is used. By saying that an object is in a quantum state, we mean that there is a list (a catalogue, in Schrödinger's language) or, which is the same, a wave function, a state vector, a density matrix containing the information about the possible results of measurement on this object. In the general case, the results of measurement differ from time to time even if the object is prepared in the same quantum state. Hence, the state vector should give statistical information, i.e., distribution functions for the results of measurement.

As a simple example, consider the state vector for a system with two orthogonal basic states, $|1\rangle$ and $|2\rangle$. For instance, these can be energy states. The state of the object is described by the state vector (wave function)

$$|\Psi\rangle = \alpha|1\rangle + \beta|2\rangle\,, \tag{1}$$

where α and β are complex numbers. In other words, the total state is given by a linear superposition, and the square absolute values of the amplitudes α and β are equal to the probabilities of finding the system in the corresponding states ($|\alpha|^2 + |\beta|^2 = 1$). As a result of measurement, the coherent superposition (1) is destroyed and reduced to a new state, which is determined by the type of measurement. For instance, an attempt to find the system in state $|2\rangle$ leads to its perturbation by the measurement device. At the moment of the measurement, the reduction (projection) takes place,

$$|\Psi\rangle \Rightarrow |2\rangle\langle 2|\Psi\rangle \Rightarrow |2\rangle\,, \tag{2}$$

so that after the measurement the system is driven into state $|2\rangle$ and the initial state is destroyed [1].

A superposition state should be distinguished from a mixed state, which is described by the density matrix

$$\rho_{\mathrm{mix}} = |\alpha|^2|1\rangle\langle 1| + |\beta|^2|2\rangle\langle 2| \,. \tag{3}$$

In fact, state (3) is a classical state, since a system in a mixed state can be discovered either in state $|1\rangle$ or in state $|2\rangle$, while in the superposition state (1), the system can be simultaneously discovered in two states. This principal feature of a superposition state manifests itself in the interference terms of its density matrix

$$\rho = |\Psi\rangle\langle\Psi| = |\alpha|^2|1\rangle\langle 1| + |\beta|^2|2\rangle\langle 2| + \alpha\beta^*|1\rangle\langle 2| + \alpha^*\beta|2\rangle\langle 1| \,. \tag{4}$$

In order to stress the unusual nature of superposition states, Schrödinger suggests an example disturbing to our common sense. Following Schrödinger, suppose that a steel chamber contains a flask with poison that can be broken by means of some mechanism triggered by the radioactive decay of a single atom. The box also contains a cat (initially alive), which can die as a result of the atom's decay. Similarly to the atom whose state is a superposition of the decayed and non-decayed states, the state of the cat is also given by the superposition of the states of an alive cat, $|\uparrow\rangle$, and a dead cat, $|\downarrow\rangle$: $|\Psi\rangle = L|\uparrow\rangle + D|\downarrow\rangle$. Since quantum superposition states are quite frequently observed for microscopic systems, such as atoms and molecules, but never observed for macroscopic systems, there must be some effect destroying the Schrödinger cat states for macroscopic systems. This effect, which is called decoherence, is considered below. Note that the problem of pertaining superposition (Schrödinger cat) states for mesoscopic systems is a crucial problem, and its solution will give rise to many applications of quantum information.

In our further consideration, we use the superposition state describing a single-photon beam with a given wave vector, or a single-photon state, $|1_{\mathrm{photon}}\rangle$. The polarization state of the radiation with a given wave vector can be represented by a set of two quantum mechanical oscillators, each of them corresponding to one of the two orthogonal polarizations (Fig. 2). Denoting the eigenstates of the oscillator with vertical polarization as $|n\rangle_{\updownarrow}$ and the eigenstates of the oscillator with horizontal polarization as $|m\rangle_{\leftrightarrow}$, we introduce two basic vectors,

$$|1\rangle_{\updownarrow}|0\rangle_{\leftrightarrow} = |\updownarrow\rangle \,, \qquad |0\rangle_{\updownarrow}|1\rangle_{\leftrightarrow} = |\leftrightarrow\rangle \,,$$

so that any single-photon state can be decomposed as

$$|1_{\mathrm{photon}}\rangle = a|\updownarrow\rangle + \beta|\leftrightarrow\rangle \,. \tag{5}$$

[1] Note that measurement, i.e., interaction with a macroscopic measurement device, is an irreversible process in principle. During this process, the state of the measured object changes (reduction takes place). Reduction, like other physical processes, has its own characteristic time scale, specific for each individual measurement. However, the process of reduction is very short, so the question of its internal dynamics, i.e., of the possibility to 'see it with one's own eyes', is usually ignored, although in some measurements, for instance, in quantum tomography of ultrashort pulses, it is of course of interest.

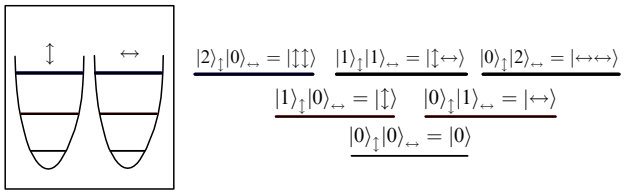


Figure 2. A light beam with a fixed wave vector is equivalent to two harmonic oscillators corresponding to two orthogonally polarized modes of the electromagnetic field. A single-photon state of this beam is given by a superposition of two energy-degenerate states of polarized photons $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$. A two-photon state of this beam is in the general case a superposition of three energy-degenerate states, two of them representing pairs of photons with equal polarizations , $|\updownarrow\updownarrow\rangle$ and $|\leftrightarrow\leftrightarrow\rangle$, and the third one representing a pair of orthogonally polarized photons, $|\updownarrow\leftrightarrow\rangle$.

Note that there is a certain ambiguity in the notion of a superposition state. Indeed, state (5) with $\alpha = \beta = 1/\sqrt{2}$ is a superposition state if considered in the basis of vertical and horizontal polarizations, i.e., measured by means of polaroids oriented horizontally and vertically. At the same time, this state $(|\updownarrow\rangle + |\leftrightarrow\rangle)/\sqrt{2}$ can be considered as one of the basic states of the pair:

$$|\nearrow\rangle = \frac{|\updownarrow\rangle + |\leftrightarrow\rangle}{\sqrt{2}} \,, \quad |\searrow\rangle = \frac{|\updownarrow\rangle - |\leftrightarrow\rangle}{\sqrt{2}} \,, \tag{6}$$

which corresponds to a measurement with the polarizers oriented at 45° and 135°. In this case, it evidently cannot be considered as a superposition state. Therefore, any quantum state is a superposition one since it is a superposition state in any basis where it is not a basic vector.

2.2 Entangled states

In addition to superposition states, Schrödinger considers the so-called entangled states, which describe the state of a composite system whose parts can be spatially delocalized. States of two systems could serve as examples of entangled state: the state of a field and the atom emitting it (Fig. 3) or a quantum system formed by two single-photon beams with different wave vectors (Fig. 4). Each state of such a photon pair can be represented as a superposition of four basic states,

$$|1_1 + 1_2\rangle = C_{\updownarrow\updownarrow}|\updownarrow\rangle_1|\updownarrow\rangle_2 + C_{\leftrightarrow\leftrightarrow}|\leftrightarrow\rangle_1|\leftrightarrow\rangle_2 + C_{\updownarrow\leftrightarrow}|\updownarrow\rangle_1|\leftrightarrow\rangle_2 + C_{\leftrightarrow\updownarrow}|\leftrightarrow\rangle_1|\updownarrow\rangle_2 \,. \tag{7}$$

Figure 3. As an example of an entangled state, consider the state of a composite system: two-level atom – field. Suppose that the atom is crossing the area of interaction with the field, for instance, a cavity. After a short period of interaction, the atom and the field become spatially separated. However, the state of the whole system stays entangled: the state of the atom is strictly correlated with the state of the field, $|\Psi\rangle = |\mathrm{atom}\rangle_1|\mathrm{field}\rangle_1 + |\mathrm{atom}\rangle_2|\mathrm{field}\rangle_2$. Note that the lifetime of such entangled state may be much larger than the interaction time.

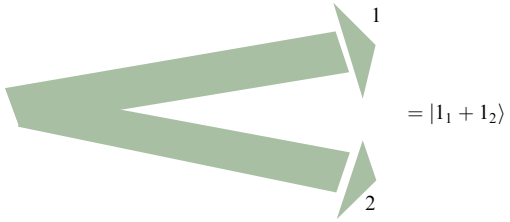


Figure 4. Two single-photon beams forming entangled photon pairs.

In the general case, the photon from the first beam is connected with the photon from the other one, since the total state vector is not given by the product of the single-photon state vectors. This connection, which is much stronger than in the case of classical correlation, manifests itself in experiments with photon pairs in Bell states. Bell suggested these states in 1964 [4] in relation to the EPR paradox. The states

$$|\Phi^+\rangle = \frac{|\updownarrow\rangle_1|\updownarrow\rangle_2 + |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2}{\sqrt{2}}\,, \tag{8a}$$

$$|\Phi^-\rangle = \frac{|\updownarrow\rangle_1|\updownarrow\rangle_2 - |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2}{\sqrt{2}}\,, \tag{8b}$$

$$|\Psi^+\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 + |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}}\,, \tag{8c}$$

$$|\Psi^-\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}} \tag{8d}$$

form the basis of the Bell states. Each one of these entangled states has a remarkable property: as soon as some measurement projects one of the photons onto a state with definite polarization, the other photon immediately also becomes polarized. For instance, in the case of $|\Psi^{\pm}\rangle$ states, if one of the photons is registered with the polarization $\leftrightarrow$, the other one turns out to have the orthogonal polarization $\updownarrow$. How can a measurement over one particle have an instant effect on the other one, possibly placed at a large distance? Einstein, as well as many other outstanding physicists, did not accept this viewpoint. In his definition, this meant 'the action of ghosts at a distance'. However, this behavior of entangled states has been demonstrated in numerous experiments [5, 6].

Entangled states have another paradoxical property, which was pointed out by Schrödinger in Ref. [1]. According to one of his principles, complete information about the state of the total system still does not give us complete information about the states of its parts. Suppose that we are going to find out the state of a particle in one of the pairs (8), say, in Eqn (8d). Then we have to average the density matrix of the pure, i.e., the most determinate, state

$$|\Psi^-\rangle = \frac{|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2}{\sqrt{2}}$$

over the states of the second particle. The resulting density matrix of the first particle,

$$\rho^{(1)} = \mathrm{Sp}_2\left(|\Psi^-\rangle\langle\Psi^-|\right) = \underbrace{\left(|\updownarrow\rangle_{11}\langle\updownarrow| + |\leftrightarrow\rangle_{11}\langle\leftrightarrow|\right)/2}_{\text{mixture}} \tag{9}$$

is apparently the density matrix of a mixed state, which is not maximally determinate.

2.2.1 How can one generate entangled states? Entangled photon pairs can be obtained experimentally via cascade decays in atomic systems [7] or parametric processes involving resonant fluorescence where two pump photons give birth to a pair of entangled photons ω_1 and ω_2, $2\omega_0 \to \omega_1 + \omega_2$. The quantum correlation for such photons has been predicted theoretically in Ref. [8] and observed experimentally in Ref. [9]. Recently, the possibility of obtaining entangled states for massive particles, atoms, has been demonstrated in experiment [10]. At present, the most popular source of entangled photons is spontaneous parametric decay (spontaneous parametric down-conversion) in crystals with quadratic nonlinearity [11, 12]. In this process, an ultraviolet pump photon decays into a pair of red photons with approximately equal energies, so that the energy and momentum conservation laws are satisfied, $\hbar\omega_\mathrm{p} = \hbar\omega_\mathrm{s} + \hbar\omega_\mathrm{i}$, $\hbar\mathbf{k}_\mathrm{p} = \hbar\mathbf{k}_\mathrm{s} + \hbar\mathbf{k}_\mathrm{i}$, where $\hbar\omega_j$ and $\hbar\mathbf{k}_j$ $(j = \mathrm{p}, \mathrm{s}, \mathrm{i})$ are the energy and momentum, respectively, of the initial (p) and the two output photons, called the signal (s) photon and the idler (i) photon. By using crystals with quadratic nonlinearity and type-II phase matching (Fig. 5), one can easily obtain polarization-entangled states in the directions 1 and 2, which are determined by the intersections of phase matching cones for ordinary and extraordinary photons (Fig. 5b). In these directions, one can observe Bell states of the form (8) [13].

2.2.2 How can one measure (project) entangled states? A Bell state can be distinguished from the other Bell states due to their different symmetry. Among the four states (8), the first three have bosonic symmetry since transmutation of particles

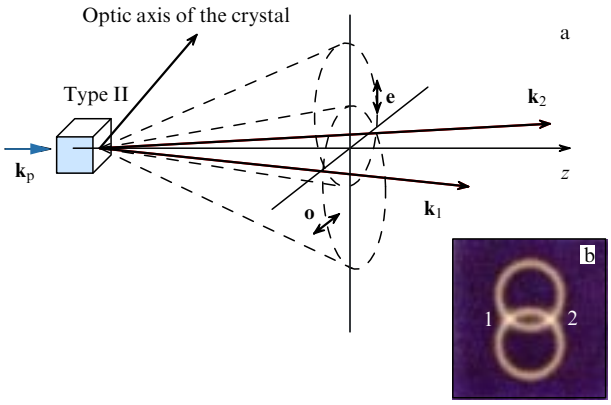


Figure 5. (a) Momentum conservation inside the crystal, also called 'phase matching', is achieved due to the crystal birefringence, which allows the dispersion to be compensated. As a result, the idler and signal photons form a rainbow of colored cones where conjugated photons are emitted in opposite directions with respect to the pump beam. In the case of type-I phase matching, the signal and idler photons have the same linear polarization, which is orthogonal to the pump polarization, and their cones are concentric with the pump beam. In the case of type-II phase matching, conjugated pairs are formed by a photon with extraordinary polarization and a photon with ordinary polarization. In this case, the cones of signal and idler photons have different axes. For uniaxial negative crystals, like BBO, the axis of the cone of extraordinary photons lies between the pump beam and the optic axis, while the axis of the cone of ordinary photons is on the opposite side of the pump beam (all the axes and the pump beam are in the same plane). (b) The image of down-converted light emitted by the crystal. Numbers 1 and 2 denote the directions in which polarization-correlated pairs are emitted. In these directions, there is no definite polarization; all we know is that the polarization is different for beams 1 and 2.

1 and 2 does not change the signs of their wave functions. The last state (8d) is fermionic: transmutation of 1 and 2 changes the sign of its wave function. This specific feature of the state $|\Psi^-\rangle = (|\updownarrow\rangle_1|\leftrightarrow\rangle_2 - |\leftrightarrow\rangle_1|\updownarrow\rangle_2)/\sqrt{2}$ also reveals itself in the intensity interference of beams 1 and 2 (Fig. 6). In Figure 6, both detectors click only if the entangled photon pairs are in the fermionic polarization state $|\Psi^-\rangle$. This is a well-known feature of two-photon interference on a beam splitter [14]: in the case of a spatially symmetric wave function, the beamsplitter sends both particles into the same output beam, while in the case of a spatially antisymmetric wave function, the two particles are directed into different output beams. Photons have bosonic statistics; therefore, conservation of the total symmetry requires that the spatial part of the polarization-fermionic wave function $|\Psi^-\rangle$ should be antisymmetric. A measurement distinguishing the fermionic state from the four states (8) is called a Bell state measurement (BSM) .

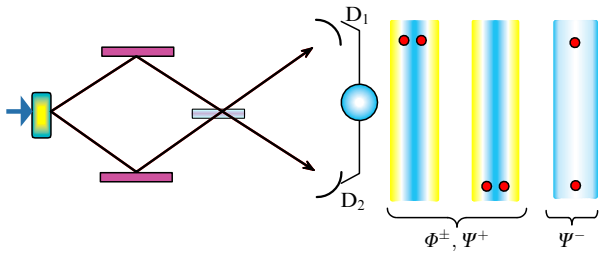


Figure 6. Scheme for observing intensity interference. Polarization-entangled beams emitted by the crystal are mixed on a 50% beamsplitter and registered by two detectors. Photocounts from the detectors are fed to the coincidence circuit. For each photon from any beam, there are two possibilities, either to be reflected or to be transmitted by the beamsplitter. The probability of a photocount is given by the square absolute value of the sum of the corresponding quantum amplitudes. The unitary transformation performed by the nonpolarizing beamsplitter concerns only the spatial part of the photon wave function. Photons are bosonic particles; therefore, the spatial part of the wave function is symmetric for the bosonic polarization states $|\Phi^\pm\rangle$, $|\Psi^+\rangle$ and antisymmetric for the fermionic state $|\Psi^-\rangle$. Two-photon interference on a beamsplitter demonstrates that two photons are directed by the beamsplitter into the same beam for the case of a symmetric wave function and into different beams for the case of an antisymmetric wave function. Hence, a coincidence of photocounts from two detectors projects the state of a photon pair onto the fermionic state $|\Psi^-\rangle$.

2.3 The impossibility of cloning quantum states

Since the measurement device destroys the initial quantum state, one can consider a quantum state as a very sensitive object that 'keeps secret' all information about itself. The uncertainty principle is one of the manifestations of this ability. Another typical manifestation is the theorem about the nonclonability of a quantum object [15]. Cloning means creation of an exact copy of an object with the conservation of it's initial (and unknown) state.

Suppose that we have a device for cloning photons. This device reproduces photons with given properties (photons in a given state). If we mean polarization states, the effect is described by the transformation

$$|\mathrm{R_I}\rangle|\updownarrow\rangle \Rightarrow |\mathrm{R_{FV}}\rangle|\updownarrow\updownarrow\rangle\,,$$

$$|\mathrm{R_I}\rangle|\leftrightarrow\rangle \Rightarrow |\mathrm{R_{FH}}\rangle|\leftrightarrow\leftrightarrow\rangle\,,$$

where $|\mathrm{R_I}\rangle$ is the initial state of the cloning device, $|\mathrm{R_{FV}}\rangle$, $|\mathrm{R_{FH}}\rangle$ are its final states after cloning photons with vertical and horizontal polarizations. In other words, instead of a single photon with a given polarization we obtain two photons with the same polarization (Fig. 2). However, if we try to clone a photon with a polarization that is neither horizontal nor vertical, for instance, $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$, then the transformation will be

$$|\mathrm{R_I}\rangle\left(\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle\right) \Rightarrow \alpha|\mathrm{R_{FV}}\rangle|\updownarrow\updownarrow\rangle + \beta|\mathrm{R_{FH}}\rangle|\leftrightarrow\leftrightarrow\rangle\,. \quad (10)$$

Even under the condition of equality $|\mathrm{R_{FV}}\rangle$ and $|\mathrm{R_{FH}}\rangle$, the transformed state does not represent two photons polarized at the angle $\varphi = \arctan\beta/\alpha$. Indeed, creation of a single photon polarized at the angle $\varphi = \arctan\beta/\alpha$, i.e. at the state $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$ could be realized by applying the creation operator $b_\varphi^+ = \alpha\hat{a}_V^+ + \beta\hat{a}_H^+$ to vacuum, where $\hat{a}_\mathrm{V}^+$, $\hat{a}_\mathrm{H}^+$ are creation operators for the photons polarized vertically and horizontally. They correspond to the right and the left harmonic oscillators in Fig. 2. Two photons with the same polarization can be obtained from the vacuum by twice applying this creation operator:

$$\frac{(\hat{b}_\varphi^+)^2}{\sqrt{2}}|0\rangle = \alpha^2|\updownarrow\updownarrow\rangle + \beta^2|\leftrightarrow\leftrightarrow\rangle + \sqrt{2}\alpha\beta|\updownarrow\leftrightarrow\rangle\,. \quad (11)$$

For all nonzero α, β, state (11) does not coincide with the field part of state (10), i.e., a single quantum object cannot be cloned.

3. Quantum teleportation

In the end of 1997, Anton Zeilinger and his colleagues [16] performed an experimental realization of teleportation, the dream of science fiction novelists. The term 'teleportation' means that an object disappears at some place and appears at another place, at some distance. Although the idea of quantum teleportation, i.e., transporting a quantum state from one object to another one, was suggested by Charles Bennett and colleagues in 1993 [17], it was the experiment [16] and another experiment following it [18] that attracted public attention.

From the classical viewpoint, teleportation means gaining all possible information about the properties of an object and then transposing these properties onto the reconstructed object. However, this procedure is forbidden in the quantum world because of the above-formulated postulates of projection and destruction of state during measurement. There exists another method of passing a quantum state from one object to another. Briefly, transmission of an unknown quantum state from Alice to Bob (traditional names used in quantum cryptography) is performed as follows:

Alice has a particle in some unknown quantum state $|\psi\rangle$. 'Teleportation' means that Alice destroys the state $|\psi\rangle$ at her location but some particle at Bob's location is put into the same state ($|\psi\rangle$). Neither Bob nor Alice get information about the state $|\psi\rangle$; moreover, Bob does not know that some state was teleported onto his particle. In order to tell Bob about the teleportation, Alice should use a classical information channel.

In this scheme, the principal role is played by photon pairs in entangled states. They provide the quantum information channel between Alice and Bob. Suppose that particle 1 (a

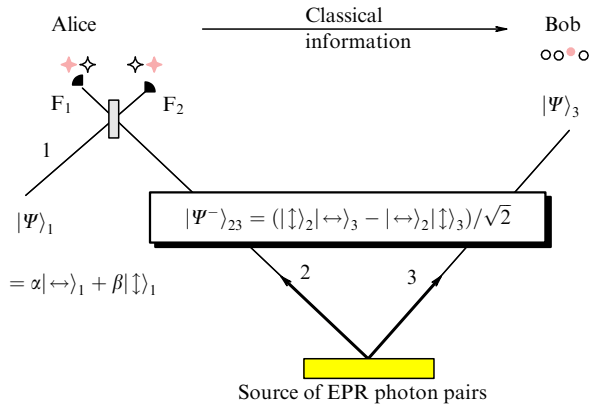


Figure 7. Principal scheme of teleportation. Alice is going to transpose the state of particle 1 onto some particle at Bob's station. Alice and Bob get photons 2 and 3, which form an EPR pair in the entangled state $|\Psi^-\rangle_{23}$. Alice performs the Bell state measurement over particles 1, 2. This way she also projects the state of particle 3 at Bob's station. In one case of four, detectors F_1 and F_2 'click' simultaneously, so that Alice knows that the state of particle 3 becomes the same as the initial state of photon 1, i.e., that teleportation of the state $|\Psi\rangle_1$ occurs. Alice can tell Bob about this through the classical channel. Moreover, if Bob gets the information through the classical channel and performs an additional unitary transformation over his particle, the state $|\Psi\rangle_1$ will be teleported with 100% probability after each Bell state measurement performed by Alice.

photon), which is to be teleported by Alice, is initially in the polarization state $|\psi\rangle_1 = \alpha|\updownarrow\rangle_1 + \beta|\leftrightarrow\rangle_1$ (Fig. 7). Alice is connected with Bob by means of photon pairs prepared by an EPR source in entangled states

$$|\Psi^-\rangle_{23} = \frac{|\updownarrow\rangle_2|\leftrightarrow\rangle_3 - |\leftrightarrow\rangle_2|\updownarrow\rangle_3}{\sqrt{2}}\,. \tag{12}$$

Photons 2 are sent to Alice and photons 3 are sent to Bob. The joint state of photons 1 and 2 meeting at Alice's station is the product of $|\Psi\rangle_1$ and $|\Psi^-\rangle_{23}$,

$$\begin{aligned}|\Psi\rangle_1|\Psi^-\rangle_{23} = {} & |\Psi^-\rangle_{12}\frac{\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3}{2} \\ & + |\Psi^+\rangle_{12}\frac{-\alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3}{2} \\ & + |\Phi^+\rangle_{12}\frac{-\beta|\leftrightarrow\rangle_3 + \alpha|\updownarrow\rangle_3}{2} \\ & + |\Phi^-\rangle_{12}\frac{\beta|\leftrightarrow\rangle_3 + \alpha|\updownarrow\rangle_3}{2}\,.\end{aligned} \tag{13}$$

Consider the wave function (13) for three particles, two of them belonging to Alice and one to Bob. If Alice projects the states of the particles 1 and 2 onto the state $|\Psi^-\rangle_{12}$, then the state of particle 3 at Bob's station is immediately reduced to the state of the first particle, $|\Psi\rangle_3 = \alpha|\leftrightarrow\rangle_3 + \beta|\updownarrow\rangle_3$. In other words, by measuring Bell states formed by mixing photons 1 and 2 on a beamsplitter and by registering the coincidences of photocounts from the detectors F_1 and F_2, Alice performs an immediate reduction of photon 3 to the initial state of photon 1, i.e., teleportation! Several features of quantum teleportation deserve additional comments.

(1) The teleportation procedure does not violate the nonclonability theorem for a single quantum object. As soon as Alice performs the Bell state measurement, photon 1 becomes a component of the polarization-entangled pair of photons 1, 2. Hence, it is not an individual particle any more. Its initial state $|\Psi\rangle_1$ is destroyed.

(2) Quantum information can be passed from photon 1 to photon 3 at any distance. At present, the largest achieved distance between entangled photons is about 10 kilometers.

(3) At the moment of measurement, Alice is aware of the teleportation going on, while Bob is not. Indeed, teleportation can occur without passing Bob any information about it. Moreover, Alice may not know the state of photon 1 transmitted by her.

(4) A classical information channel is required for informing Bob about the teleportation of the unknown state onto photon 3.

(5) Suppose that Alice performs a complete Bell state measurement and identifies, in addition to the fermionic state, the three bosonic states, each of them occurring with probability 25%, and sends this information to Bob through the classical channel. Then, by means of an appropriate operation performed over photon 3, Bob can transform its state into the initial state of photon 1 for any result of Alice's measurement. If this procedure is omitted and Alice only projects for the fermionic state, then teleportation occurs only in 25% of all trials. This fact has been demonstrated experimentally in Ref. [16].

The experimental scheme used in Ref. [16] is shown in Fig. 8. Correlated photons 2–3 connecting Alice with Bob were generated via type-II parametric down-conversion in a nonlinear crystal from a UV femtosecond pulsed pump. Photon 1 whose state was to be teleported was generated from the reflected pump beam. The Bell state measurement for photons 1 and 2 was performed by mixing these photons on a beamsplitter and registering coincidences of photocounts from detectors F_1 and F_2. The polarization properties of Bob's photon were analyzed by means of a polarizing beamsplitter and two detectors D_1 and D_2.

Teleportation was experimentally demonstrated by registering coincidences of photocounts from detectors F_1 and F_2 and one of Bob's detectors (triple coincidences). Suppose that photon 1, which is to be teleported, is polarized at 45°, and Bob's polarizing beamsplitter is sending −45°-polarized light

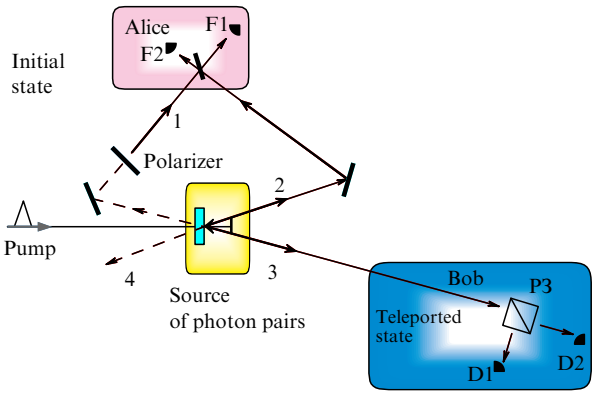


Figure 8. Scheme of the quantum teleportation experiment [16]. Correlated photons 2 and 3 connecting Alice and Bob were produced by a nonlinear crystal via type-II parametric down-conversion from a UV femtosecond pulsed pump. The reflected pump generated photon 1 whose state was to be teleported and photon 4, which was used as a time reference. The Bell state measurement for photons 1 and 2 was performed by mixing them on a beamsplitter and then registering by the detectors F_1 and F_2. The polarization properties of Bob's photon were analyzed by means of a polarizing beamsplitter and two detectors D_1 and D_2.

to detector D_1 and $+45°$-polarized light to detector D_2. Then a coincidence of photocounts from F_1 and F_2 means that photon 3 is polarized at $+45°$, i.e., a photocount comes from D_2 and not from D_1. Hence, if triple coincidence counting rates $(D_1F_1F_2)$ and $(D_2F_1F_2)$ are registered as functions of the delay between photons 1 and 2, which is varied by shifting the mirror reflecting the pump, one should expect a gap with complete suppression of coincidences for $(D_1F_1F_2)$ and no dependence for $(D_2F_1F_2)$. Outside the teleportation domain, i.e., for delays between photons 1 and 2 so large that these photons hit F_1 and F_2 independently, the probability of triple coincidences is constant and equal to $50\% \times 50\% = 25\%$ (50% is the coincidence probability of photons 1 and 2 and 50% is the probability that photon 3, which in this case has no definite polarization, hits D_1 or D_2.) The experimental data obtained in Ref. [16] confirmed these predictions, both for the case of photon 1 polarized at 45° (Fig. 9a, b) and for the case of photon 1 polarized at $-45°$ (Fig. 9c, d). Teleportation was also performed for photons in superpositions of these polarization states: 0°, 90°, and circularly polarized photons.

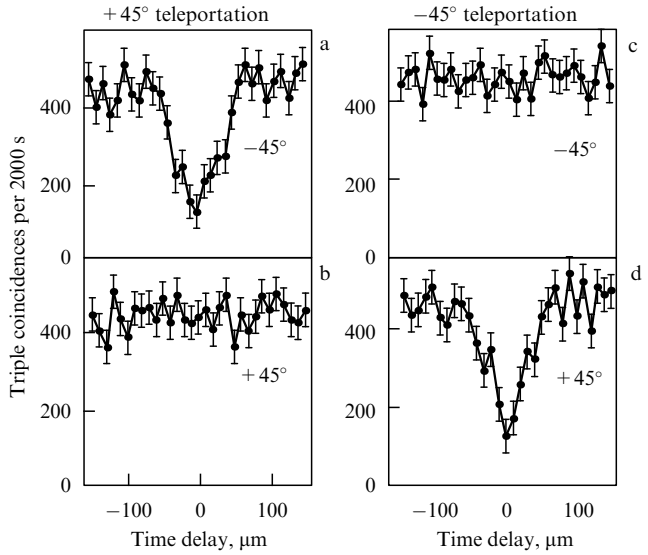


Figure 9. Triple coincidence counting rates, $D_1F_1F_2(-45°)$ and $D_2F_1F_2(+45°)$, as functions of the delay between photons 1 and 2. The delay is varied by moving the mirror reflecting the pump pulses. The teleported photon 1 is polarized at $+45°$ (a, b) and at $-45°$ (c, d).

Realization of quantum state teleportation opens new possibilities for transmitting 'fragile' superposition states at large distances without loss of coherence. Solving this problem is crucial for the development of quantum computers. In addition, quantum teleportation is important in connection with some fundamental problems, such as, for instance, information exchange in complex spatially separated molecular structures, including biological ones.

The importance of paper [16] and the subsequent experiments[2] [18] is clear from the fact that since, the information aspects of quantum mechanics have been treated not only as leading to 'gedanken experiments' but also as 'practically important'. In addition, the teleportation experiments demonstrated once again that the 'classical' interpretation of quantum mechanics, which is based on the notions of 'superposition' and 'reduction' and which so far predicted correctly the *results of experiment*, was confirmed once again. As any quantum mechanical measurement fixes one of the possible realizations arising from the originally prepared state, Alice's measurements ensure that Bob gets photon 3 in the original state of photon 1. This is only one of the possibilities that appear from the initial state of the three photons, two of which (2 and 3) are originally in an entangled state generated by a common source. Here one should not forget that in quantum mechanics, the possibilities for arbitrary initial states are not necessarily described by positive probability distribution functions, i.e., their description cannot be reduced to classical probability theory. Of course, an alternative interpretation, based on classical probabilities, can be found for certain experiments, measurements, and states. At present, it is unclear, however, if this is possible in the general case. The modern state of this point can be found in Ref. [19].

4. Quantum cryptography

One of the most practical aspects of quantum information is quantum cryptography. The aim of cryptography is secret information exchange between two stations (Alice and Bob), so that any attempt of eavesdropping messages or breaking the secret code would be unsuccessful. This problem is almost solvable by modern methods of classical cryptography, for instance, in the framework of a 'symmetrical' cryptosystem based on a secret code.

In this system, Alice and Bob, and nobody else, have a secrete code, i.e., a sequence of random numbers, for instance, decimals,

$$K = \{12793\ 41169\ 42357\ldots\}.$$

According to some fixed rule, each alphabet letter is put into correspondence to a decimal number. Alice sends to Bob a message where each letter is replaced by a corresponding number. In this simple form, the procedure has no defense and can be easily broken. The obtained message in the form of a sequence of numbers

$$P = \{73997\ 68279\ 65867\ldots\}$$

is then encoded, i.e., a digit from the code is added to each digit from the message. As a result, digits in the junior decimal orders form the cryptogram

$$C = \{85680\ 09338\ 07114\ldots\},$$

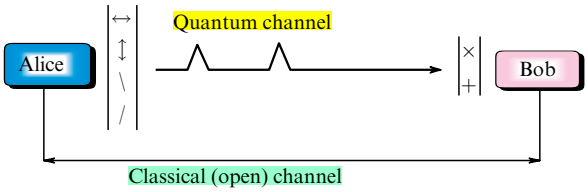
which can be transmitted through an open channel (telephone, etc.). After receiving the cryptogram, Bob decodes it using the code K and obtains the message P. Note that the above sequences K, P, and C are taken from a real message sent by Che Guevara from Bolivia to F Castro Ruz in Cuba in 1967 [20].

In 1994, C E Shannon, using information theory, proved that such a cryptosystem is absolutely secret if the secret code is truly random and is used only once [21]. However, the

[2] When the present paper was under consideration of the Editorial Board, two experimental papers appeared in which non-conditional quantum teleportation was realized using squeezed bimodal optical fields [Furusawa A et al. *Science* **282** 706 (1998)] and the total quantum teleportation of the hydrogen atom magnetic states to the states of chlorine atom inside a single trichloroethylene molecule was performed (Nielsen M A, Knill E, Laflamme R, http: //xxx.lanl.gov/archive/quant-ph/ 9811020).

practical realization of this system faces serious difficulties. One of them is the creation and transmission of a large secret code for each message. These difficulties could be avoided by using some physical channel, which would be secret due to certain physical principles. This is exactly what quantum physics provides us with.

The possibility of organizing such a secret channel is based, like quantum cryptography, on the impossibility of cloning a single quantum object. If the secret code is transmitted via the states of single quantum particles, it cannot be eavesdropped, since any measurement would destroy quantum states. This event can be registered by using a special agreement (protocol) between Alice and Bob. One of the possible protocols can be organized by encoding polarization states of photons in two alternative non-orthogonal bases [3] [22]. The secret code is transmitted in two stages (Fig. 10).



No	Actions								Secrecy
1	A → B	1	0	0	1	0	0	1	1	secret
		↕	/	↔	\	↔	↔	↕	↕	quantum channel
2	B measures	+	+	×	×	+	×	×	+	open channel
		↕	↕	/	\	↔	/	/	↕	secret
3	A → B: type of measurement A → B: correct	√			√	√			√	open channel
4	A and B create a code	↕			\	↔			↕	secret
		1			1	0			1	

Figure 10. Procedure of quantum cryptography with polarization encoding.

1. First, Alice and Bob discuss the encoding (for instance, photons with polarizations 0° and 45° correspond to a zero and photons with polarizations 90° and 135° to a unity). Then Alice randomly changes polarization of photons sent to Bob through the quantum channel.

2. Bob measures the polarizations of received photons using an analyzer with the orientation randomly changed from 0°, 90°(+) to 45°, 135°(×).

3. Through the open channel, Bob tells Alice which measurement he performed over each photon, and Alice tells him if the choice was correct or not.

4. Leaving in the whole sequence only correctly chosen measurements, Alice and Bob create a secret code.

If an eavesdropper tries to find out the secret code, he would cause discrepancies between the codes obtained by Alice and Bob. Alice and Bob can discover this by comparing randomly chosen digits of the code; if the errors exceed the level determined by the detectors, they conclude that there has been an attempt at eavesdropping.

Another possible protocol for transmitting the quantum code is provided by phase modulation with interferometric detection [22] based on the interference of a single photon with itself in a setup formed by two Mach–Zehnder interferometers (Fig. 11). A photon sent by Alice can hit Bob's detector within one of three separate time intervals, depending on its path. The first time interval corresponds to the case 'short arm of interferometer A – short arm of interferometer B'. The second interval corresponds to two indistinguishable cases 'short arm of A – long arm of B' and 'long arm of A – short arm of B'. The third interval corresponds to the case 'long arm of A – long arm of B'.

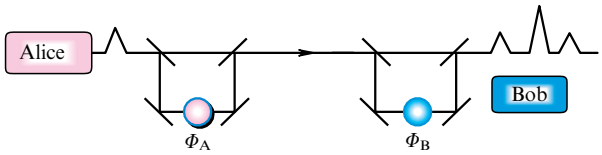


Figure 11. The scheme of quantum cryptography with phase modulation and interferometric detection.

Due to the indistinguishability of the two paths of photons fitting the second interval, there must be interference depending on the phase difference Φ_A and Φ_B for modulators monitored by Alice and Bob. Indeed, the probability of detecting a photon within the second interval is

$$P_B \propto \cos^2\left(\frac{\Phi_A - \Phi_B}{2}\right).$$

Hence, if Alice and Bob use the phases $(\Phi_A, \Phi_B) = (0.3\pi/2)$ for the zero-bits and $(\Phi_A, \Phi_B) = (\pi/2, \pi)$ for the unity-bits, they obtain an analogue of the polarization encoding described above.

At present, the most convenient medium for the quantum channel is an optical fiber. Through an optical fiber, cryptograms can be sent at distances over 100 km. Since optical fiber has considerable birefringence fluctuations, the 'polarization version' of quantum cryptography is connected with certain difficulties and interferometric detection is preferable.

Experimental realization of quantum cryptography is possible under some additional requirements: small losses in the quantum channel [optical fiber has low losses in the IR range for wavelengths 1.3 μm (0.3 dB/km) and 1.55 μm]; operation of photodetectors in the photon counting regime (for the chosen wavelength of 1.3 μm, existing Ge or InGaAs avalanche photodiodes under some conditions [23] can be used for this purpose); and no amplifiers introduced into the channel. (From the nonclonability theorem, it follows that an amplifier in the quantum channel leads to the same effect as an attempt at eavesdropping.)

At present, there are two experimental setups for quantum cryptography [23, 24]. In Ref. [24], the quantum code was transmitted through a standard optical fiber (Swiss Telecom) under Lake Geneva over a distance of 23 km. The length of the code transmitted during the 11 hours of the session was 20 kbit; there were 1% of errors, mostly caused by the germanium photodiode.

[3] Each of the digits is encoded by two polarizations to guarantee secrecy. Using only one basis leaves only one quantum channel for transmitting the code from Alice to Bob. But in this case, even if Alice transmits a random code, Bob has no possibility to check whether it is correct or broken by eavesdropping attempts.

Above, we considered only a single type of protocol for classical and quantum cryptography. There exist many other protocols. One of them, RSA, is the most popular cryptosystem with open code transmission. It was suggested by R Rivest, A Shamir, and L Adelman [25] (the abbreviation RSA is formed from their initials). In this protocol, two secret codes are used: one code for encoding and another code for decoding. In addition, there is an auxiliary code transmitted through open channels, which is the product of large prime numbers (containing more than 200 digits). The secrecy is ensured by the fact that factoring large numbers is a complicated computational problem, and with modern facilities, it cannot be solved in a reasonable time. Recently, an attempt to solve the mathematical part of this problem led to the suggestion of a fast procedure that could be realized in so-called quantum computers. For these devices to be constructed, a consolidation of efforts in many fields of physics is required: quantum optics, solid state physics, laser physics, and spectroscopy.

5. Quantum computations and computers

5.1 Reversible and irreversible classical processors

Before presenting the basic principles of quantum computations and quantum computers, for a more clear demonstration of their peculiarities we briefly describe some aspects of the work of ordinary, classical computers. Classical computers as devices for calculations must operate with numbers. The simplest device which can represent numbers should have two stable states. For instance, conductors can be in two states: when there is no current, which corresponds to 0, and when the current is present, which corresponds to 1. Such devices can perform operations over numbers written in binary codes. For example, the natural number 9 is written in the binary code as $1001 = (1 \times 2^3) + (0 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$, and numbers are summed according to the table

$$0 + 0 = 0,$$
$$0 + 1 = 1,$$
$$1 + 0 = 1,$$
$$1 + 1 = 0 \text{ (1 in the next digit, 'in the mind')}.$$

At present, there are a lot of devices that can perform this operation. As illustrative example consider a mechanical version of a summing device (Fig. 12). This device consists of gates and connecting channels. Balls can move along the channels under the action of gravity. When moving, the balls turn the gates into one of two possible positions; the T-state of a gate corresponds to 0, while the turned λ-state corresponds to 1. There are two types of gates in the device: gates A and C shown by the gray hatching, which fix the state of the channel in which they are located, and the gates B shown by the black color, which are logical gates of the summation of two bits. Indeed, each of the gates B has one input channel (to the left) and two output channels (to the right). Among the output channels, the lower one corresponds to the bit of carrying to the next digit and the upper one is used for ball removal. If the presence of a ball at the input of gate B corresponds to 1 and its absence to 0, this logical unit acts according to Table 1. This indeed is equivalent to the operation of two-bit summation if the state of the input B is treated as the first bit and the second term is the initial state of gate B. Then the final state of the gate B together with the final state of the carrying bit is the result of the summation. Combining such logical gates in a network by connecting the bit-carrying channel to the input of the next-digit logical gate, we obtain a processor for summing arbitrary numbers (Figs 12a–c).

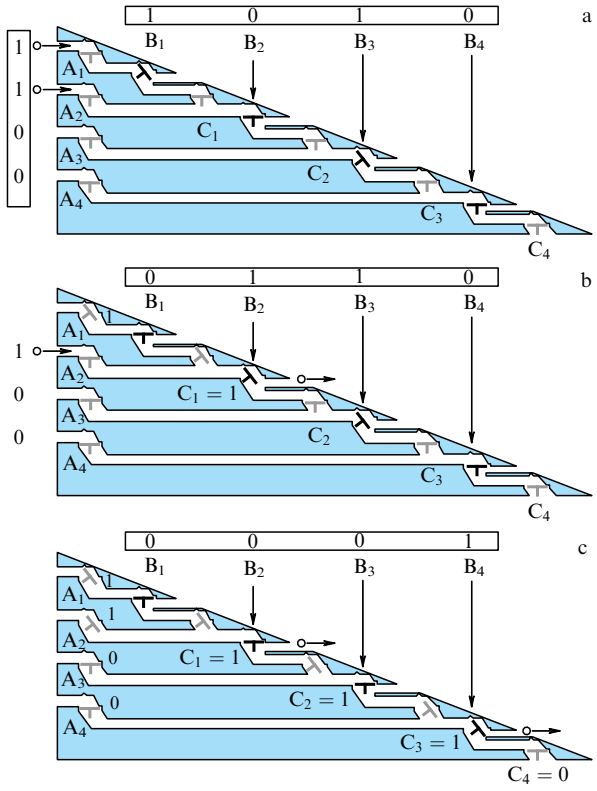


Figure 12. Mechanical scheme of a summing processor with balls. The device consists of gates and connecting channels. Balls can move along the channels under the action of gravity. When moving, the balls turn the gates in one of two possible positions. A T-state of the gate corresponds to 0, and the turned λ-position corresponds to 1. There are gates of two types: gates A and C, which are denoted by gray hatching, record the state of the channel where they are installed, and gates B, colored black, serve as logical gates of two-bit summation. (a) The original state of the processor: the states of the gates (B_4, B_3, B_2, B_1) 'encode' the number 5 = 101; the balls at the input 'prepare' another number 3 = 11. (b) The state of the summing processor after the action of a ball from the first digit: the number 1 is written down in the register $\{A_i\}$, and the number 110 (5 + 1) in the register $\{B_i\}$. (c) The final state of the summing processor after the action of a ball from the second digit: the register $\{A_i\}$ contains the initial number 11. The register $\{B_i\}$ is turned into the state corresponding to the sum 101 + 11 = 1000 (5 + 3 = 8).

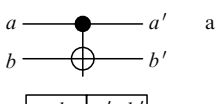
Table 1.

Initial state of the gate B entrance (ball — 1, no ball — 0)	Initial state of gate B (T = 0, λ = 1)	Final state of gate B	Final state of the bottom output channel (bit-carrying channel)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

The operation of such a processor has an important feature. This processor will perform the summation operation even without the gates A and C. In this case, the operation of the summator will be irreversible. Indeed, for the transformation 'two inputs → one output' (the initial state

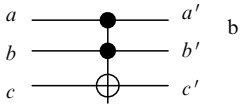
of gate B input, the initial state of gate B input — the final state of gate B), the information at the output is not sufficient for determining what was at the input (cf. the second and the third rows in Table 1) and thus to reverse the operation. However, in 1973, Charles Bennett [26] showed that all logical operations needed to design a computer (there are only $4^2 = 16$ of them for logical gates 'two inputs → one output') can be made reversible. For the summation operation, the initial bit states should be conserved, i.e., transformations like $(a, b) \to (a' = a, b' = a + b)$, where the prime means the final input or output state, should be used. In 1980 Tom Toffoli found [27] how one can describe reversible calculations using the traditional language of Boolean logical gates, such as AND, OR, etc., but having the property of reversibility. One such logical gate, which was shown later to be very important for quantum calculations, acts like a controlled NOT (reversible XOR). The bit b (target bit) changes its state if and only if the state of the control bit a corresponds to 1; the state of the control bit remains unchanged (Fig. 13a). Toffoli also showed that an arbitrary reversible processor can be constructed using only a single logical gate, Toffoli's universal three-bit gate (Fig. 13b). In this logical block, the state of the target bit (c) changes if and only if both variable control bits (a and b) correspond to 1. Figure 12 can be also used to demonstrate the reversibility of the classical summator. Adding to the consideration the gates A and C, which are used to fix the states of the inputs (A_i) and carrying bits (C_i) in each digit, we get a reversible summator. Indeed, if we invert this device around the horizontal axis (Fig. 12c) and consecutively 'let in' the balls which fell into the evacuation channels, the final state of the device after the balls have passed coincides with the initial one.

A logical network (Fig. 14) demonstrating the time evolution of bit states can equivalently describe the operation of such a reversible summation processor. The idea of a quantum processor is a single step ahead of such a logical network of bit states. R Feynman made this step [28, 29] in eighties when he realized that reversible computation networks can operate, instead of classical bit states, with quantum states of systems governed by reversible Hamiltonian dynamics. This time can be considered as a beginning of quantum computers history.



a

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



b

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Figure 13. (a) Graphic representation and *truth table* for an elementary controlled-NOT gate: bit b (the target bit) changes its state if and only if the state of the control bit a corresponds to 1, with the control bit state remaining unchanged. Each horizontal line represents the state of a single bit changing in time from left to right. The symbols on two lines connected with the vertical line mean the joint action of two gates on these bits. Clearly, the *truth table* for this logical gate, which is also called EXCLUSIVE OR (XOR), corresponds to the table of two-bit addition if in the latter the carrying bit is not taken into account. (b) The graphic representation and the *truth table* for Toffoli's three-bit logical gate, which is universal for constructing reversible Boolean logic. Its action reduces to changing the target bit c state provided that both invariable control bits (a and b) correspond to 1. Each horizontal line represents the state of a single bit, which changes in time from left to right. The symbols near the three lines connected with the vertical line mean joint action of the three gates on these bits.

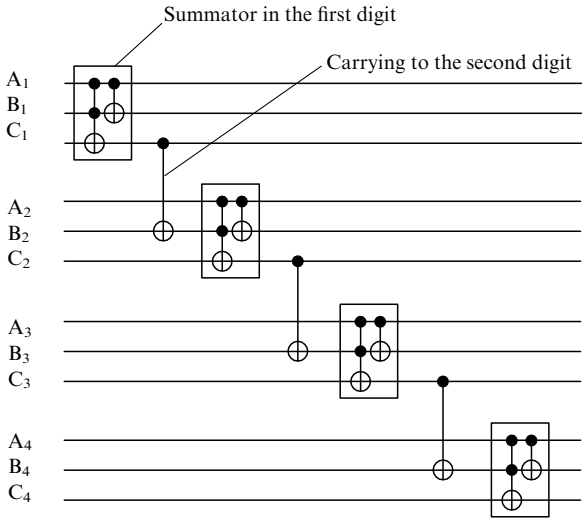


Figure 14. Logical scheme of a reversible summator with the mechanical scheme shown in Fig. 12. The horizontal lines correspond to the states of the digit bits of two numbers to be summed, (A_4, A_3, A_2, A_1) and (B_4, B_3, B_2, B_1), as well as to the carrying bits, (C_4, C_3, C_2, C_1). The digit-*summing blocks* represent an operation that can be performed by a ball falling on the gates B_i in the mechanical scheme: the gate B_i changes its state provided that a ball is present in the channel A_i; if the state of the gate C_i before the interaction corresponded to 1, the ball is carried into the next digit along the transmission channel changing the state of the gate C that originally had the state 0. *Carrying blocks* perform the controlled-NOT operation by changing the state of gate B_{i+1} with a ball that entered the $i + 1$th summing gate from the carrying bit channel C_i.

5.2 Quantum computers

Quantum computers are physical devices performing logical operations over quantum states by means of unitary transformations that do not violate quantum superpositions. In the most schematic form, the work of a quantum computer can be represented as a sequence of three operations:

(1) recording (preparation) of the initial state;

(2) computation (unitary transformations performed over the initial states);

(3) reading out the result (measurement, or projection, of the final state).

(1) A normal numerical computer operates with bits, Boolean variables, that take values 0 and 1. At each stage of calculation, each bit has a definite value, which can be measured. At the first stage, the initial data should be written into the register (a set of bits), each bit having a definite value (0 or 1).

A quantum computer operates with quantum states. The simplest state that plays the role of a bit in a classical computer is a qubit, or a quantum information bit, which is the state of a quantum system with two basic states $|0\rangle$ and $|1\rangle$. The general state of this system is a superposition

$$|q\rangle = c_0|0\rangle + c_1|1\rangle\,,$$

which is something different from a Boolean 0 or 1. A qubit is a quantum superposition of two numbers, zero and unity! Qubits can be realized in any physical system with two quantum states: photon polarization states, electronic states of isolated atoms or ions, spin states of nuclei, lower states of quantum dots, and so on.

The advantage of operating with qubits can be noticed even at the first stage of computation. If the initial number is written into a classical register consisting of w bits, w operations are required, since for each bit, the values of 0 or 1 should be set. As a result, only a single number of length w is written. After w unitary operations performed over each qubit in a quantum register (a device consisting, for instance, of w quantum dots, see Fig. 15), a coherent superposition of all $Q = 2^w$ states of the total system, quantum register, is prepared. This way, instead of a single number, we obtain 2^w possible readings of the register, a coherent superposition of all possible numbers written in it. Naturally, this property can be used for quantum parallel calculations.

(2) Applying unitary transformations, which play the role of logical operations, to the prepared quantum states we obtain a quantum processor. The role of connections (wires) is played by qubits and the role of logical blocks (gates) constituting the whole computation process is played by unitary transformations. This concept of quantum processing and quantum gates together with universal quantum gate (analogous to the Toffoli's gate in classical computation) have been proposed by D Deutsch in 1989 [30]. Recently, it was shown that one- and two-bit gates are sufficient for obtaining all the necessary set of transformations [31–34]. In particular, these are the negation operation NOT (quantum analog of gates A and C in classical summator on balls),

$$\hat{T}_{\mathrm{NOT}} = |0\rangle\langle 1| + |1\rangle\langle 0|\,, \tag{14}$$

acting on a single qubit and transforming its state into

$$\hat{T}_{\mathrm{NOT}}|0\rangle = |1\rangle\,, \qquad \hat{T}_{\mathrm{NOT}}|1\rangle = |0\rangle\,,$$

and the controlled-NOT, or exclusive-OR (XOR) operation (quantum analog of gates B in classical summator on balls considered above),

$$\hat{T}_{\mathrm{XOR}} = |0\rangle_{11}\langle 0|\hat{I}_2 + |1\rangle_{11}\langle 1|\hat{T}_{2\mathrm{NOT}}\,, \tag{15}$$

acting on two qubits so that the first of them stays unchanged and the second one changes depending on the state of the first one. For instance,

$$\hat{T}_{\mathrm{XOR}}\left(\alpha|0\rangle_1 + \beta|1\rangle_1\right)|0\rangle_2 = \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2\,, \tag{16}$$

i.e., the operation $\hat{T}_{\mathrm{XOR}}$ transforms superposition states into entangled ones and vice versa. A quantum analog to the logical Toffoli gate (controlled – controlled NOT) (Fig. 13b) acts on three qubits according to the relation

$$\begin{aligned}\hat{T}_{\mathrm{Toffoli}}&\left(\alpha|0\rangle_1 + \beta|1\rangle_1\right)\left(\gamma|0\rangle_2 + \delta|1\rangle_2\right)\left(\mu|0\rangle_3 + \nu|1\rangle_3\right)\\ &= \left[\alpha|1\rangle_1\left(\gamma|0\rangle_2 + \delta|1\rangle_2\right) + \beta\gamma|0\rangle_1|0\rangle_2\right]\left(\mu|0\rangle_3 + \nu|1\rangle_3\right)\\ &\quad + \beta\delta|1\rangle_1|1\rangle_2\left(\mu|1\rangle_3 + \nu|0\rangle_3\right).\end{aligned} \tag{17}$$

Quantum logical blocks combined together and acting on qubit states in a certain order form a quantum network. Taking the scheme of the reversible summing processor as an example (see Fig. 12) and considering two-level systems instead of gates, with interactions corresponding to unitary transformations (15)–(17), one obtains (see Fig. 14) the simplest quantum network, a summator.

(3) The operation of reading the result in a classical computer does not differ from any other operation in the course of computation. Computation can be stopped at any stage, with the intermediate result read and then computation resumed. In a quantum computer, this is different. The final result of a quantum computation is the state of the quantum register after all unitary transformations. This state is a coherent superposition of all states possible for this register. Evidently, we cannot obtain all probability amplitudes C_j in the decomposition of this superposition state. According to quantum theory, all that we can get from this single quantum object is a set of quadratic forms $\sum_{i,j} C_i C_j^* R_{ij}$ given by the measurement of some physical value corresponding to the operator R. It is also clear that the final result of a quantum computation would fluctuate from run to run. However, even

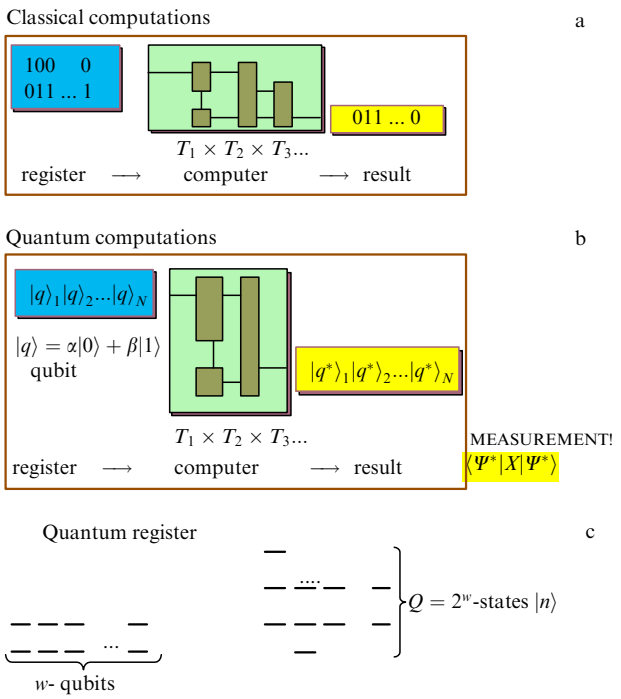


Figure 15. Quantum computers. These are physical devices performing logical operations on quantum states by means of unitary transformations, so that quantum superpositions are not destroyed during the computation. Schematically, the work of a quantum computer (b) can be represented as a sequence of three procedures: recording (preparation) of the initial state; computation (unitary transformations performed on the initial state); and output of the result (measurement, projecting of the final state). In contrast to a normal numerical computer (a), which operates with bits, Boolean variables taking values 0 or 1, a quantum computer operates with qubits, quantum information bits, which are states of a quantum system with two basic states, $|0\rangle$ and $|1\rangle$. Physically, qubits can be realized with any systems that have two quantum states. These can be polarization states of photons, electronic states of isolated atoms or ions, spin states of nuclei, lower states in quantum dots, and so on. The result of a quantum computation should be treated as some probability distribution and measured in many repeated trials. (c) A quantum register is formed by the states of several qubits. For w qubits in a register, the number of states of the register is $Q = 2^w$.

under such conditions, quantum computers can essentially accelerate calculations for some mathematical problems.

5.2.1 Quantum computers and mathematical problems. When Feynman first noticed the possibility of constructing a processor based on quantum mechanical principles [29], it was not clear in what mathematical problems it would have advantages over usual processors. The first realistic example was found by P W Shor in 1994 [35]. Shor suggested an algorithm for factoring a large n-digit number; the proposed algorithm allowed the calculation time to be reduced from the exponential value $\exp n^{1/2}$, which is necessary in the case of classical computers, to the polynomial value (n^2) required by a quantum computer. Factoring integers belongs to the class of mathematical problems where the solution is sought from among an exponentially large number of candidates.

The problem of factoring can be reduced to finding the period of an auxiliary function. This function is the residual of dividing a power function a^x by an integer number N:

$$f_N(x) = a^x \bmod N\,.$$

For instance, for $a = 11$, $N = 15$, the values of $f_N(x)$ corresponding to $x = 0, 1, 2, 3$ are equal to 1, 11, 1, 11, respectively, i.e., the period of the function $11^x \bmod 15$ equals 2. Further, the procedure of finding prime divisors is reduced to the following operations: $11 \pm 1 = 10, 12$; $15 - 10 = 5$; $15 - 12 = 3$.

Shor showed that the procedure of finding the period of a periodic function is considerably simplified by using a quantum computation. The following operations should be performed (Fig. 16):

(A) Preparation of two registers, one of them for the arguments (the x-register) and another one for the values of the periodic function, for instance, the integer-valued function $f_N(x) = a^x \bmod N$. Let the number of qubits in the x-register be w, then this register contains $Q = 2^w$ possible states, which will be further denoted as $|n\rangle_x$ (Fig. 16). The number of qubits can be exponentially smaller than the period r of the function $f_N(x)$. The y-register contains the same number of bits. Let us denote its basic states as $|m\rangle_y$. The x-register, initially in the ground state, is put, after rotating each qubit by 45°, into the state of uniform superposition

$$\frac{1}{\sqrt{Q}}\left(|0\rangle_x + |1\rangle_x + |2\rangle_x + |3\rangle_x + \ldots + |Q-1\rangle_x\right)|0\rangle_y\,.$$

Further, by performing an appropriate unitary transformation U_f, the state is transformed into the entangled state of two registers,

$$\frac{1}{\sqrt{Q}}\left(|0\rangle_x|f_N(0)\rangle_y + |1\rangle_x|f_N(1)\rangle_y + |2\rangle_x|f_N(2)\rangle_y + |3\rangle_x|f_N(3)\rangle_y + \ldots + |Q-1\rangle_x|f_N(Q-1)\rangle_y\right). \quad (18)$$

This state is schematically shown in Fig. 16b as some periodic function, so that each point in the plot corresponds to a pair of integer numbers $[n, m = f_N(n)]$ denoting the term $|n\rangle_x|f_N(n)\rangle_y$ in the sum (18); with n on the horizontal axis, m on the vertical.

(B) Next, a discrete Fourier transform is performed over the states of the x-register. The corresponding unitary transformation of the basis,

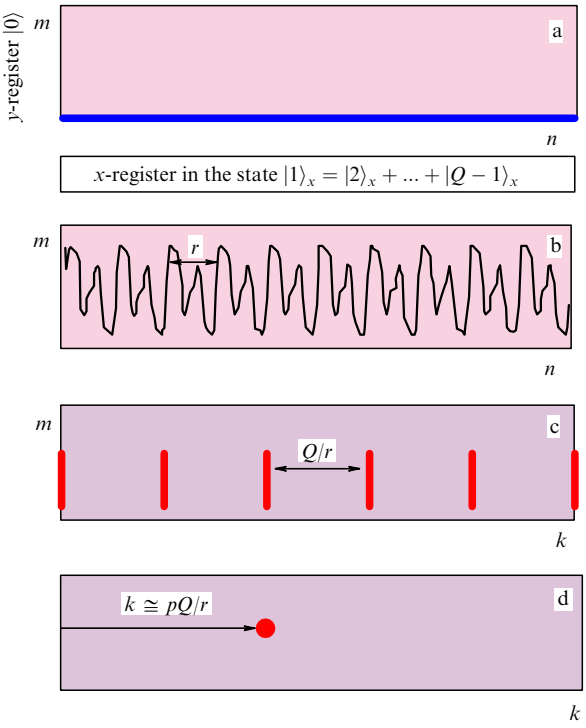


Figure 16. Obtaining the period of a periodic function by means of a quantum computation. (a) Preparation of independent states of two registers, x and y. The abscissa correspond to the numbers n of the basic states $|n\rangle_x$ in the x-register, the ordinates denote the numbers m of the states $|m\rangle_y$ in the y-register. The line shows the numbers of the states in two registers that form the initial state. (b) Entangled state of two registers (18), with the numbers of connected states of registers x, y forming a discrete periodic function $m(n)$ with the period r. (c) The same state but with the basis of the x-register changed by the discrete Fourier transform (19). Due to the function periodicity, only states with numbers k localized in the vicinity of Q/r form the entangled state in the new basis. (d) Because of this localization, several measurements of the x-register state are sufficient for determining the period r.

$$T_{\mathrm{FT}} = \frac{1}{Q}\sum_{n=0}^{Q-1}\sum_{k=0}^{Q-1}\exp\left(\frac{2\pi i k n}{Q}\right)|k\rangle_{xx}\langle n|\,, \quad (19)$$

applied to the state (18), leads to a new state of both registers,

$$\sum_{k=0}^{Q-1}\sum_{m=0}^{r}\Delta_{km}|k\rangle_x|f_N(m)\rangle_y\,, \quad (20)$$

where the amplitude of each state in the x-register,

$$\Delta_{km} = \sum_{l=0}^{G_m}\exp\frac{2\pi i k(lr+m)}{Q} = \exp\frac{2\pi i k m}{Q} \times \frac{\exp(2\pi i k r G_m/Q) - 1}{\exp(2\pi i k r/Q) - 1}\,, \quad (21)$$

has a maximum at $k = pQ/r$ (Fig. 16c). Evidently, it is supposed that the total number of states, Q, is not multiple of the period r. In Eqn (21),

$$G_m = \left[\frac{Q}{r}\right] + \theta(Q \bmod r - m)\,,$$

i.e., G_m is either equal to the number of periods r in the total number of states Q or exceeds this number by unity, depending of whether the residual of dividing Q by r is larger than m or not.

(C) The result of measurement (or measurements) of the state of the x-register is approximately given by the ratio Q/r, since the amplitudes Δ_{km} are localized near these values (Fig. 16c). Hence, we obtain the period r.

Note that applying a discrete Fourier transform to the problem of finding an unknown period is analogous to measuring the period of some lattice using the diffraction of X-rays or neutrons. However, if the problem of factoring a 200-digit number were solved by means of diffraction, we would need a crystal with period 10^{200} A and size 10^{400} A and radiation with a wavelength 1 A. Naturally, this is hardly possible.

There exist other mathematical problems where solutions are sought from among an exponentially large number of candidates. Recently, a method of solving another problem was proposed, with the time of calculation reduced dramatically by using quantum computation. This is the problem of searching among the elements of a database with each element answering YES/NO to a query [36]. At the same time, a lot of similar problems are still waiting for solutions. These are, for instance, combinatorial problems and, in particular, the salesman problem [37]: to find the shortest path connecting n points with known distances between pairs of points, so that each point is passed only once. Other problems of this type are calculations of the optimal way of supplying shops with goods, consumers with electricity, building ring electric communications and so on. Searching for new algorithms of solving these problems by means of quantum computations is one of the most significant problems of quantum information theory. Another significant problem is the correction of errors generated in the course of computation. Since quantum states are very sensitive to external perturbations, the correction of errors in quantum computers is much more important than in classical ones [38, 39].

5.2.2 Quantum computers and physical problems. At present, the creation of a quantum computer is first of all a physical problem. One of the difficulties is the fast decay of superposition states, with their turning into mixed states. This process is called decoherence, and the analysis of its nature resolves the Schrödinger cat paradox (see Section 6). The effect of decoherence imposes restrictions on the physical elements used in optical computers: the coherence times of quantum states should exceed the time of calculation. Hence, there are two possible ways of avoiding the decay of coherence: to find a quantum system isolated from the surroundings or to increase the coherence time artificially.

Possible types of isolated quantum systems are summarized in Table 2. Isolation of field quantum systems, modes of electromagnetic field, is possible in high-Q microcavities of optical [40] and microwave [41] ranges. Such cavities, with sizes of several millimeters, allow coherence of superposition quantum states to be maintained for times from seconds to microseconds, with the number of photons per mode varying from unity to a hundred [42]. Another promising method of field isolation is using surface modes like 'whispering galleries' mode on microspheres of synthetic silicon [43]. For those modes, it was possible to achieve a quality factor of order $10^9 - 10^{10}$, which corresponds to a coherence time 1 – 0.1 μs [44]. A novel isolation method is using three-dimensional periodic dielectric structures, called photonic crystals [45, 46], which perfectly 'confine' photons from certain frequency bands. The localization of photons in photonic crystals is so high that a single atom interacting with a photonic crystal should manifest suppression of spontaneous decay and inversion-free generation of coherent monochromatic sub-Poissonian radiation [47, 48]. Among several candidates to photonic crystal materials, the most perspective at present is synthetic opal [49, 50].

Table 2. Localization of single quantum systems.

Field	Matter
Microcavities: *optical* [40]; *microwave* [41, 42]	***Beams*** ***Ion traps:***: *Paul trap* [51]; *end-cap* [52, 53]; *quadrupole ring traps* [54]
	Laser traps [57, 58]
Cavities for 'whispering gallery' modes [43, 44]	***Naturally isolated systems***: *molecules in amorphous and polycrystalline matrices* [60, 61];
Photonic crystals [45 – 50]	*impurities in crystals* [62]; *molecules in biological structures* [63 – 65] (*investigation method: single-molecule spectroscopy* [66 – 68])
	Quantum dots [69]
	Nuclear spins of molecules [70 – 72]

The isolation of single massive particles, such as atoms, molecules, and ions, was historically preceded by one-dimensional isolation in beams (Table 2). Among other isolation (localization) methods, let us mention the following:

(1) Quadrupole ion traps, called Paul traps [51] of various configurations, which can keep a single ion (the endcap trap [52] illuminated by laser beams [53]) or several ions (ring quadrupole traps [54]). The last sort of trap is also considered as a possible realization of quantum registers [55]. A two-bit quantum computer was successfully realized in an experiment with a single cooled beryllium ion [56].

(2) Optical traps for neutral atoms [57, 58]. Observation of Bose – Einstein condensation [59] suggests that this object can be also useful for quantum computation.

(3) Methods of matrix isolation of molecules in polycrystalline and amorphous media [60] and gels [61], impurity centers in crystals [62], and molecules in spatially organized structures such as DNA [63], proteins [64], photosynthetic antenna complexes [65]. Considerable progress in the study of isolated molecular systems is due to the fast development of single-molecule experimental and theoretical spectroscopy [66 – 68].

(4) Quantum dots [69].

(5) As a promising object for quantum computation, one can use spin molecules, which are considerably isolated from the surrounding due to the screening effect. In this case, coherence times can reach several seconds. For a large number of molecules, for instance, kept in solution, a quantum register would have 2^n states, where n is the number of spins in a single molecule and not the number of molecules in the solution [70]. Probably, the molecules can be considered as a natural elementary quantum computer. The first experimental realizations of logical blocks have been performed using the nuclear magnetic resonance of three nuclear spins (proton and carbon spins of trichloroethylene) [71].

First quantum algorithm has been demonstrated in Ref. [72] on nuclear spins of chloroform molecule. This quantum algorithm is analogous to well-known game with coins [4]. Note that there is a principal difference between computations on quantum objects distributed in some medium and isolated quantum objects. This is analogous to the difference between an experiment with an ensemble of objects and an ensemble of experiments with a single object.

Among other physical problems connected with the idea of quantum computations, let us mention the search for physical processes realizing logical operations. The XOR operations can be performed by means of single ions interacting with microwave fields in cavities [73, 74] or ions oscillating in traps [55, 56]. There is a promising method of dynamical monitoring of quantum tunneling by means of laser radiation [75].

If optical fields are used not only for transmission but also for logical operations, it is important to develop methods of measuring their quantum states, which can have forms of complex superpositions. These possibilities are provided by quantum tomography [76] and various methods of quantum non-demolition measurements [77]. In devices operating with photon-number field states, such as, for instance, nodes of a quantum information network, one faces a set of problems connected with sub-Poissonian field generation [78]. Experimental methods of generating sub-Poissonian fields are based on using either unitary transformations [79] or non-unitary (projection) transformations [80–85].

Sometimes, the quantum object used for computation cannot be properly isolated, and the errors caused by its interaction with the environment destroy quantum coherence. In these cases, one can use various methods of quantum error correction, such as increasing the number of information channels with further correction based on some protocol [38, 39], regularization of the interaction with the environment [86–90], feedback methods [91–94], and passive methods [95]. All these methods solve the decoherence problem, which was illustrated so brightly by the Schrödinger cat paradox [1].

6. The problem of decoherence

There are some general features of the decoherence process, which manifests itself as a fast transformation of a pure state into a mixed state because of the interaction between the quantum system and the surrounding. As an isolated quantum object, let us consider a harmonic oscillator, which can represent a field in a cavity or an ion oscillating in a trap. Let the initial state of the oscillator be a superposition of two coherent states, both corresponding to the same complex amplitude. We obtain an example of the Schrödinger cat state (Fig. 17). To make this object explicit, one can use Wigner's quasiprobability function

[4] In a well-known game, your partner has a coin in his hand and you are asked to determine if this coin has two different sides or they are the same. Clearly, after having seen different sides of the coin, you give the answer. But is it possible to give the correct answer having seen only one side of the coin? Modeling such a situation with nuclear spin states of a chloroform molecule, the authors of paper [72] gave the answer in one run of the quantum processor. They used the spin states of hydrogen nuclei as an indicator of which side of the coin has been looked at (the spin up or down), and the spin states of carbon nucleus as an indicator of the result of observation.

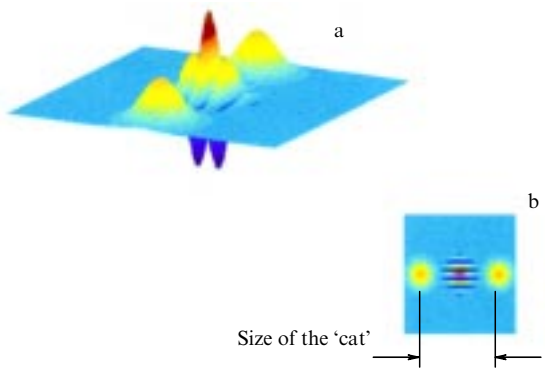


Figure 17. (a) Wigner function of the superposition formed by two coherent states with the phases differing by π. The two peaks correspond to the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$. The distance between the peaks determines the size of the Schrödinger cat, i.e., indicates how macroscopic the state is. (b) The projection of the Wigner function. A specific feature of the Wigner function for the state $|\alpha\rangle + \exp(i\theta)|-\alpha\rangle$ is the interference part at the center of the phase plane. Because of the quantum nature of the state, there are points where its Wigner function takes negative values.

$$W(\beta)=\frac{1}{\pi^2}\int d^2\xi\,\mathrm{Sp}\left\{\hat{\rho}\exp\left[\xi(\hat{a}^+-\beta^*)-\xi^*(\hat{a}-\beta)\right]\right\}. \tag{22}$$

Its two-dimensional plot contains complete information about the wave function of the object represented by the harmonic oscillator (a photon, a phonon, or any other quantum system). For classical states, this function is equal to the joint probability distribution function in the variables 'coordinate x-momentum p' ($\beta = x + ip$). In particular, for the state

$$|\psi_+\rangle = N\left(|\alpha\rangle + \exp i\theta|-\alpha\rangle\right),$$
$$N^{-2} = 2\left[1+\cos\theta\exp(-2|\alpha|^2)\right], \tag{23}$$

the Wigner function $W(\beta)$ has two maxima localized at points $\beta = \pm\alpha$ and indicating the probabilities of finding the system in the states $|\alpha\rangle$ or $|-\alpha\rangle$. In addition, there is an interference structure at $\beta = 0$, which for some arguments takes negative values. This structure appears due to quantum interference terms $|\alpha\rangle\langle-\alpha|\exp(-i\theta) + |-\alpha\rangle\langle\alpha|\exp i\theta$ in the density matrix of the state (23). It is this structure that indicates that the state is nonclassical.

Relaxation caused, for instance, by the escape of photons from the cavity with the rate γ, leads to a specific change in the state of the oscillator: first, the interference part disappears, and the superposition state turns into a mixed state, and then the mixed state gradually becomes the vacuum state (Fig. 18). Moreover, the rate at which the interference terms $t_{\mathrm{decoh}}^{-1} = 2\gamma|\alpha|^2$ decay is higher, the larger the size of the state (22), determined by the amplitude α. This feature of relaxation, first pointed out by W H Zurek [86], explains why superposition states are easily observed in the microscopic world but are never observed for macroscopic objects, i.e., why we never observe the superposition of a dead cat and an alive cat. However, this fact still gives no solution to the problem of avoiding decoherence. To find the solution, the relaxation process should be investigated in detail.

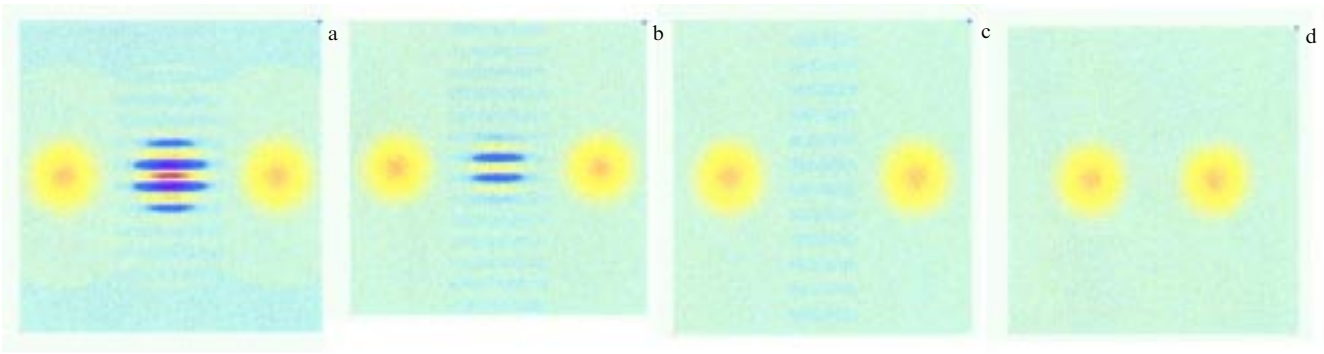


Figure 18. Evolution of the Wigner function for a quantum harmonic oscillator with damping. The initial state of the oscillator is $|\alpha\rangle + \exp(i\theta)|-\alpha\rangle$. The Wigner function is shown at $t = 0$ (a), $1/16\gamma$ (b), $1/4\gamma$ (c), $1/\gamma$ (d); $\alpha = 2$. Decoherence manifests itself in the fast decay of the interference part of the Wigner function in the course of relaxation.

6.1 Relaxation as a nonunitary evolution of a state. Quantum reservoirs engineering

Any kind of relaxation is due to the interaction of the system with the reservoir, which is an object with many degrees of freedom and a broad continuous energy spectrum. This provides a unidirectional transfer of excitation from the system to the reservoir. A standard model for the reservoir is a large number of harmonic oscillators with distributed eigenfrequencies ω_i and creation and annihilation operators b_i^+, b_i. The states of the system and the reservoir, initially independent, become entangled because of the interaction. As a result, the initial superposition state of the system loses its individuality and becomes a mixed state. The details of this transition depend on the specific form of the interaction between the system and the reservoir. Suppose that the quantum system, represented by an oscillator, interacts with the reservoir via the Hamiltonian

$$H_{\text{int}} = A(a, a^+)\Gamma^+ + A^+(a, a^+)\Gamma\,, \tag{24}$$

where $A(a, a^+)$ is a function (nonlinear in the general case) of the creation and annihilation operators for the oscillator and $\Gamma = \hbar\sum_i g_i b_i$ is a linear function of the reservoir operators. Although Hamiltonian (24) is not universal, it still describes numerous physical situations. First, for a linear interaction, $A(a, a^+) = a$, and the relaxation is described by the equation

$$\dot\rho = \frac{\gamma}{2}(2a\rho a^+ - a^+a\rho - \rho a^+a) \tag{25}$$

for the density matrix of the oscillator a averaged over the initial vacuum state of the reservoir. The constant $\gamma = \pi\rho(\omega)|g(\omega)|^2$ is the energy relaxation rate, $\rho(\omega)$ is the density of states for the reservoir. Solving Eqn (25), we can obtain the density matrix as a function of time and predict possible results of measurements performed over the oscillator a. For instance, the initial superposition $|\psi_+\rangle = N(|\alpha\rangle + \exp i\theta|-\alpha\rangle)$ evolves, according to Eqn (25), as

$$\begin{aligned}\rho(t) = {} & \frac{1}{2}\left(|\alpha_t\rangle\langle\alpha_t| + |-\alpha_t\rangle\langle-\alpha_t|\right) \\ & + \frac{1}{2}\exp\left\{-2|\alpha|^2\left[1-\exp(-\gamma t)\right]\right\} \\ & \times\left[\exp i\theta|-\alpha_t\rangle\langle\alpha_t| + \exp(-i\theta)|\alpha_t\rangle\langle-\alpha_t|\right];\end{aligned} \tag{26}$$

this dependence describes a slow decrease in the amplitude $\alpha_t = \alpha\exp(-\gamma t/2)$ and a fast, with the rate $t_{\text{decoh}}^{-1} = 2\gamma|\alpha|^2$, transition into a mixed state.

In the general case of a nonlinear interaction between the oscillator a and the reservoir, relaxation is described by the kinetic equation

$$\dot\rho = \frac{\gamma}{2}\left([A, \rho A^+] + [A\rho, A^+]\right). \tag{27}$$

From this equation, in combination with the Hamiltonian (24), it follows that the relaxation of the oscillator a considerably depends on the form of the interaction $A(a, a^+)$. Indeed, the eigenstates $|\Psi\rangle_A$ of the interaction operator $A(a, a^+)$ stay non-perturbed by the interaction with the reservoir and form the so-called 'pointing basis' [86], which determines the specific form of the relaxational evolution. Hence, by using various forms of the interaction operator $A(a, a^+)$, one can create various 'pointing bases' and thus vary the relaxation process and, moreover, obtain various stationary states as a result of the relaxation. Several well-known examples of 'quantum reservoir engineering' are given in Table 3.

Note that replacing the harmonic oscillator by a set of N two-level systems, which represent a quantum register, one can find a subspace of the register states that is completely orthogonal to the states of the reservoir. Such states of the register would not be perturbed by the reservoir. Several

Table 3. Various'system-reservoir' interactions for quantum reservoirs engineering.

Type of interaction	'Pointing basis'	Stationary state	References
$A = a + a^+ \sim x$	Coordinate eigenstates	Vacuum	[86]
$A = a^2$	Even and odd coherent states	Vacuum	[87]
$A = (a+\alpha)(a-\alpha)$	Even and odd coherent states	Even and odd coherent states	[88–90]
$A = a^+a$	Fock states	Vacuum	[90]
$A = a(a^+a - n)$	Fock states	Fock states	[90]
$A = \exp(i\pi a^+a)a$	Yurke–Stoler superposition states	Vacuum	[91–93]

special cases have been considered in Ref. [95]. On the other hand, there is a strong correlation between the states of a single two-level atom and the reservoir, for instance, radiation. Due to this correlation, the atom dynamics can be varied by changing the state of the field. For instance, if one of the reservoir modes (a resonance mode) is initially in the Yurke–Stoler state, $|\alpha\rangle + \mathrm{i}|-\alpha\rangle$, and the other reservoir modes are in the vacuum state, the entangled nature of joint states leads to the effect of quantum instability, which manifests itself in the exponential growth of the transition dipole moment of the atom [96], instead of the usual Rabi oscillations.

6.2 Relaxation as a quantum stochastic process. Purity of conditional states

Relaxation of the oscillator a can be also considered as a result of averaging of quantum stochastic processes of excitation transfer from the oscillator a to the oscillators of the reservoir. In each process of this kind, such as, for instance, the escape of a photon from a cavity, a quantum is passed from the oscillator a to the reservoir. As a result, there is an instant change, reduction, of the state of the oscillator a. The absence of quantum exchange between the acts of reduction, which occur at random time moments, does not mean that the state of a remains constant. Indeed, the longer we wait for the next quantum to be emitted, the higher the probability that oscillator a will be in the ground state; hence, its amplitude should decrease during such periods. Such a sequence of reductions and intervals of non-unitary evolution is studied by the theory of continuous quantum measurements or quantum jumps [97–99]. In the case of relaxation with linear interaction, this sequence of random events is described by the conditional state vector of the oscillator a after transmitting exactly n quanta to the reservoir at time moments $t_1, t_2, \ldots, t_n$ belonging to the interval $[0, t)$:

$$|\psi_{\mathrm{cond}}(t)\rangle = \gamma^n S(t, t_n) a S(t_n, t_{n-1}) a \ldots a S(t_1, 0) |\psi(0)\rangle \,, \quad (28)$$

where $S(t_i, t_{i-1}) = \exp\{-\gamma a^+ a (t_i - t_{i-1})/2\}$ is a non-unitary operator of the evolution between two sequential reductions at t_{i-1} and t_i. Emission of quanta at time moments $\{t_i\}$ results in the reduction of the state. If $|\psi(0)\rangle = |\psi_+\rangle$, then this effect,

$$a\big[|\alpha\rangle \pm \exp(\mathrm{i}\theta)|-\alpha\rangle\big] = \alpha\big[|\alpha\rangle \mp \exp(\mathrm{i}\theta)|-\alpha\rangle\big] \,, \quad (29)$$

increases the relative phase θ by π, but the state remains a pure superposition state. The non-unitary evolution $S(t_i, t_{i-1})$ between quantum emissions reduces the amplitude α exponentially, so that the conditional state

$$|\psi_{\mathrm{cond}}(t)\rangle = N(\gamma\alpha)^n \big[|\alpha \exp(-\gamma t/2)\rangle + (-1)^n \exp(\mathrm{i}\theta)|-\alpha \exp(-\gamma t/2)\rangle\big] \quad (30)$$

remains pure throughout the whole evolution period, and its coherence is preserved! Conservation of purity for conditional states in the course of relaxation does not contradict the above consideration of the density matrix decoherence: if the conditional density matrix $|\psi_{\mathrm{cond}}(t)\rangle\langle\psi_{\mathrm{cond}}(t)|$ is averaged over random realizations of quantum emissions, we immediately obtain the result (26), which means that the information about the state of the system is partially lost. It is also evident that the first emission event occurring after the average waiting time equal to the decoherence time, $t_{\mathrm{decoh}} = 1/2\gamma|\alpha|^2$, is sufficient to erase the quantum interference terms.

6.3 Correcting errors by means of feedback

Relaxation considered as a quantum stochastic process also shows that although decoherence is a serious obstacle for quantum information processing, it can still be overcome. In order to correct the errors and uncertainties caused by the interaction of the quantum object with the surroundings, it is not necessary to know the state of the surroundings. It is quite sufficient to control the times of quantum emissions from the object to the surroundings and to return the system after each reduction into its initial state by means of some unitary transformation [91–93].

For the case of Yurke–Stoler coherent states $|\alpha\rangle + \mathrm{i}|-\alpha\rangle$, this protocol of error correcting should be carried out by rotating the phase of the oscillator a by 180° [91]. Then the sequence of events in the quantum stochastic process would consist of alternating stages of non-unitary evolution (the absence of emissions), reduction, and phase variation,

$$|\psi_{\mathrm{cond}}(t)\rangle = \gamma^n S(t, t_n) \exp(\mathrm{i}\pi a^+ a) a S(t_n, t_{n-1}) \times \exp(\mathrm{i}\pi a^+ a) a \ldots \exp(\mathrm{i}\pi a^+ a) a S(t_1, 0) |\psi_+\rangle \,. \quad (31)$$

Due to the correcting procedure, which can be realized by the back action on the oscillator a (Fig. 19), not only the conditional state but also the unconditional state of the oscillator, obtained by averaging over random realizations of emissions, remain pure superpositions,

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}} \big[\big|\alpha \exp(-\gamma t/2)\big\rangle + \mathrm{i}\big|-\alpha \exp(-\gamma t/2)\big\rangle\big] \,. \quad (32)$$

In this case, the only sign indicating the existence of relaxation is the exponential amplitude decay (energy relaxation).

Note that the density matrix of the state (32) satisfies an equation similar to Eqn (27):

$$\dot{\rho} = \frac{\gamma}{2} \Big(\big[A_\pi, \rho A_\pi^+\big] + \big[A_\pi \rho, A_\pi^+\big] \Big) \,, \quad (33)$$

where the nonlinear interaction operators $A_\pi = \exp(\mathrm{i}\pi a^+ a) a$ and $A_\pi^+ = a^+ \exp(-\mathrm{i}\pi a^+ a)$ belong to the class of generalized creation and annihilation operators $A_\varphi = \exp(\mathrm{i}\varphi a^+ a) a$, $A_\varphi^+ = a^+ \exp(-\mathrm{i}\varphi a^+ a)$, whose eigenvectors, generalized coherent states, have extraordinary quantum properties [92].

The experimental scheme for the proposed decoherence correction is evident [93] (Fig. 19). The inter-cavity field, initially in the Yurke–Stoler state, is continuously registered by a high-efficiency detector. From each photocount of the detector, a signal is fed through a feedback to the phase modulator, which changes the field phase by π. If this procedure is continued, the superposition state in the cavity

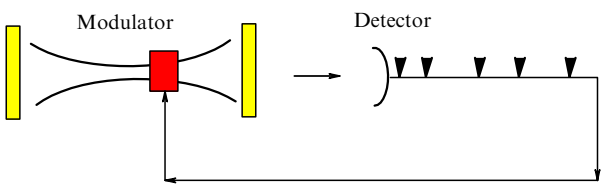


Figure 19. Slowing down decoherence by means of an error-correcting feedback. The intra-cavity field, initially in the Yurke–Stoler state, is continuously detected by a high-efficiency detector. Each photocount is converted into a signal on the phase modulator, which changes the phase of the field by π. If this procedure is repeated continuously, the superposition state is preserved as long as there are some photons in the cavity.

is conserved as long as there remain some photons in the cavity.

Suppression of decoherence by means of feedback is a universal method and can be applied to all systems with continuously controllable losses (local nodes of a quantum computer). At present, in addition to Refs [91 – 93], there are some other suggestions in this direction [94]. If the control of losses is difficult, as in the case of transmission through quantum channels, one should use quantum error-correcting methods based on duplicating transmitted qubits [38, 39].

7. Conclusions

Quantum informatics is developing remarkably fast. The 'scientific race' for new achievements in quantum information has involved, joined and enriched several fields of science, such as discrete mathematics and quantum mechanics, computer science and quantum optics. Moreover, it has given practical importance to studies that previously seemed to be far from practical applications, such as the investigation of single quantum objects: atoms and ions in high-finesse cavities and traps, molecules and impurity centers in polymer and crystalline matrices. All this stimulates such a rapid development of new approaches, methods, and materials that it is hardly possible to keep up on current publications. A useful source of information are electronic publications and e-preprints available on the Internet earlier than the corresponding hard copies [100].

In conclusion, it should be mentioned that in spite of the 'famous names' and the long period separating us from the basic paper by Schrödinger [1], the real development of quantum information, with its practical importance for human society, is being started only now. An extremely important contribution to the development of this field was made by B B Kadomtsev, whose death became known to us when this paper was under consideration by the Editorial Board. B B Kadomtsev believed that informational aspects of quantum theory must be considered in detail. His last monograph [101] is devoted to the problems of quantum information theory.

Acknowledgements. The author is grateful to the Belarus Republic Foundation for Basic Research for supporting work in the field of quantum information and to its Chairman A S Rubanov for his suggestion to write this review, to V S Burakov for an invitation to visit the seminar of the Belarus Physical Society and deliver a talk that had considerable influence on this work, to P A Apanasevich, D B Khoroshko, V N Shatokhin, A P Nizovtsev, T M Maevskaya, D S Mogilevtsev, T B Karlovich, and V A Zaporozhchenko for cooperation, and also to H Walther, P Berman, M Raymer, G Bjork, C von Borczyskowski for fruitful discussions. With gratitude, acknowledged is partial financial support of the National Science Foundation of the USA (grant NSF 9414515 'Spectroscopy of single molecules'), Volkswagen Foundation (grant 1/72 171 'Two-level systems in single-molecule spectroscopy'), INTAS (grant 96 167 'Generation of single photons and synthesis of quantum states'), and the National Scientific Council of the USA (Twinning program 'Quantum tomography and other reconstructive measurement methods in quantum optics') are acknowledged.

References

1. Schrödinger E *Naturwissenschaften* **23** 807, 823, 844 (1935) [Translated into Russian: *Uspekhi Khimii* **5** 390 (1936); translated into English: *Proc. Am. Philos. Soc.* **124** 323 (1980)]
2. Einstein A, Podolsky B, Rosen N *Phys. Rev.* **45** 777 (1935)
3. Bohr N *Phys. Rev.* **48** 696 (1935)
4. Bell J S *Physics* **1** 195 (1964)
5. Clauser J F, Shimony A *Rep. Prog. Phys.* **41** 1881 (1978)
6. Greenberger D M, Horne M A, Zeilinger A *Phys. Today* **46** (8) 22 (1993)
7. Aspect A, Grangier P, Roger G *Phys. Rev. Lett.* **47** 460 (1981)
8. Apanasevich P A, Kilin S Ya *Phys. Lett. A* **62** 83 (1977); *J. Phys. B* **12** L83 (1979)
9. Aspect A et al. *Phys. Rev. Lett.* **45** 617 (1980)
10. Hagley E et al. *Phys. Rev. Lett.* **79** 1 (1997)
11. Zel'dovich B Ya, Klyshko D N *Pis'ma Zh. Eksp. Teor. Fiz.* **9** 69 (1969) [*JETP Lett.* **9** 40 (1969)]
12. Burnham D C, Weinberg D L *Phys. Rev. Lett.* **25** 84 (1970)
13. Kwiat P G et al. *Phys. Rev. Lett.* **75** 4337 (1995)
14. Feynman R P, Leighton R B, Sands M *The Feynman Lectures on Physics* Vol. 8 (London: Addison-Wesley, 1964)
15. Wootters W K, Zurek W H *Nature* (London) **299** 802 (1982)
16. Bouwmeester D et al. *Nature* (London) **390** 575 (1997)
17. Bennett C H et al. *Phys. Rev. Lett.* **70** 1895 (1993)
18. Boschi D et al. *Phys. Rev. Lett.* **80** 1121 (1998)
19. Klyshko D N *Usp. Fiz. Nauk* **168** 975 (1998) [*Phys. Usp.* **41** 885 (1998)]
20. Bennett C H, Brassard G, Ekert A K *Scientific Am.* **267** 26 (1992)
21. Shannon C E *Bell Syst. Tech. J.* **28** 657 (1949)
22. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992)
23. Hughes R J et al. *Contemp. Phys.* **38** 149 (1995)
24. Muller A, Zbinden H, Gisin N *Europhys. Lett.* **33** 335 (1996); **33** 586 (1997)
25. Rivest R, Shamir A, Adleman L "On digital signatures and public-key cryptosystems", MIT Laboratory for Computer Science Technical Report MIT/LCS/TR-212 (1979)
26. Bennett C H *IBM J. Res. Dev.* **17** 525 (1973)
27. Toffoli T, in *Automata, Languages and Programming* (Eds J W de Bakker, J van Leeuwen) (New York: Springer, 1980) p. 632
28. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
29. Feynman R P *Found. Phys.* **16** 507 (1986) [First published in *Opt. News* **11** (February 1985); Translated into Russian *Sov. Phys. Usp.* **149** 671 (1986)]
30. Deutsch D *Proc. R. Soc. London Ser. A* **425** 73 (1989)
31. Schumacher B *Phys. Rev. A* **51** 2738 (1995)
32. DiVincenzo D *Phys. Rev. A* **51** 1015 (1995)
33. Barenco A et al. *Phys. Rev. Lett.* **74** 4073 (1995)
34. Sleator T, Weifurtner H *Phys. Rev. Lett.* **74** 4087 (1995)
35. P W Shor, in *Proc. of the 35th Ann. Symp. of the Foundations of Computer Sci.* (Ed S Goldwasser) (Los Alamitos, CA: IEEE Computer Society, 1994) p. 124
36. Grover L K *Phys. Rev. Lett.* **79** 4709 (1997)
37. Ore O *Theory of Graphs* (American Mathematical Society Colloquium Publ., Vol. 38) (Providence: Am. Math. Soc., 1962) [Translated into Russian (Moscow: Nauka, 1968)]
38. Shor P W *Phys. Rev. A* **52** R2493 (1995)
39. Ekert A, Macchiavello C *Phys. Rev. Lett.* **77** 2585 (1995)
40. Kimble H J, in *Cavity Quantum Electrodynamics* (Ed P Berman) (New York: Academic Press, 1994) p. 203
41. Raithel G et al., in *Cavity Quantum Electrodynamics* (Ed P Berman) (New York: Academic Press, 1994) p. 57
42. Davidovich L et al. *Phys. Rev. A* **53** 1295 (1996)
43. Braginsky V B, Gorodetsky M L, Ilchenko V S *Phys. Lett. A* **137** 393 (1989)
44. Collet L et al. *Europhys. Lett.* **23** 327 (1993)
45. John S *Phys. Rev. Lett.* **58** 2486 (1987)
46. Yablonovich E *Phys. Rev. Lett.* **58** 2059 (1987)
47. Kilin S Ya, Mogilevtsev D S *Laser Phys.* **2** 153 (1992)
48. Kilin S Ya, Mogilevtsev D S *Opt. Spektrosk.* **74** 974 (1993) [*Opt. Spectrosc.* **74** 579 (1993)]
49. Bogomolov V N et al. *Phys. Rev. E* **55** 7619 (1997)

50. Romanov S G, Johnson N P, De La Rue D M *Appl. Phys. Lett.* **70** 2091 (1997)
51. Fischer E *Z. Phys.* **156** 1 (1959)
52. Scharma C A et al. *Opt. Commum.* **101** 32 (1993)
53. Hoffges J T et al. *J. Mod. Opt.* **44** 1999 (1997)
54. Birkl G, Kassner S, Walther H *Nature* (London) **357** 310 (1992)
55. Cirac J, Zoller P *Phys. Rev. Lett.* **74** 4091 (1995)
56. Monroe C et al. *Phys. Rev. Lett.***75** 4714 (1995)
57. Minogin V G, Letokhov V S *Davlenie Lazernogo Izlucheniya na Atomy* (Laser Light Pressure on Atoms) (Moscow: Nauka, 1986) [Translated into English (New York: Gordon and Breach Science Publ., 1987)]
58. D J Wineland, C E Wieman, S J Smith (Eds) *Atomic Physics* **14** (New York: AIP, 1994)
59. Anderson M A et al. *Science* **269** 198 (1995)
60. T Basché, W E Moerner, M Orrit, U P Wild (Eds) *Single-Molecule Optical Detection, Imaging and Spectroscopy* (Weinheim: VCH, 1996)
61. Dickson R M et al. *Science* **274** 966 (1996)
62. Gruber A et al. *Science* **276** 2012 (1997)
63. Wennmalm S, Edman L, Rigler R *Proc. Natl. Acad. Sci. USA* **94** 10641 (1997)
64. Dickson R M et al. *Nature* (London) **388** 355 (1996)
65. Tietz C et al. *J. Chem. Phys.* (1999) (in print)
66. Pirotta M et al. *Spectroscopy Europe* **9/4** 16 (1997)
67. Kilin S Ya et al. *Phys. Rev. B* **56** 24 (1997)
68. Kilin S Ya et al. *Phys. Rev. A* **57** 1400 (1998)
69. Ekert A, Jozsa R *Rev. Mod. Phys.* **68** 733 (1996)
70. Gershenfeld N, Chuang I *Science* **275** 350 (1997)
71. Laflamme R et al. Quantum Computation/Cryptography at Los Alamos — http://qso.lanl.gov/qc/ (March 1998)
72. Chuang I L et al. *Nature* (London) **393** 143 (1998)
73. Turchette Q A et al. *Phys. Rev. Lett.* **75** 4710 (1995)
74. Kilin S Ya, Krinitskaya T B *J. Opt. Soc. Am. B* **8** 2289 (1991); *Phys. Rev. A* **48** 3870 (1993)
75. Kilin S Ya, Berman P, Maevskaya T M *Phys. Rev. Lett.* **76** 3297 (1996)
76. Leonardt U et al. *Opt. Commun.* **127** 144 (1996)
77. Braginsky V B, Khalili F Ya *Quantum Measurement* (Cambridge: Cambridge Univ. Press, 1992)
78. Rarity J G, Tapster P R, in *Quantum Optics of Confined Systems* (NATO ASI Series, Ser. E, No 314) (Eds M Ducloy, D Bloch) (Dordrecht: Kluwer Acad. Publ., 1996) p. 47
79. Kilin S Ya, Horoshko D B *Phys. Rev. Lett.* **74** 5206 (1995)
80. Golubev Yu M, Sokolov I V *Zh. Eksp. Teor. Fiz.* **87** 408 (1984) [*Sov. Phys. JETP* **60** 234 (1984)]
81. Yamamoto Y, Imoto N, Machida S *Phys. Rev. A* **33** 3243 (1986)
82. Fofanov Ya A *Kvantovaya Elektron.* **12** 2593 (1989)
83. Khoroshko D B, Kilin S Ya *Zh. Eksp. Teor. Fiz.* **106** 1278 (1994) [*JETP* **79** 691 (1994)]; *Opt. Spektrosk.* **82** 913 (1997) [*Opt. Spectrosc.* **82** 838 (1997)]
84. Yamamoto Y et al. *Prog. Opt.* **28** 88 (1990)
85. Jann A, Ben-Aryeh Y *J. Opt. Soc. Am.* **14** 11 (1997)
86. Zurek W H *Phys. Today* **44** (10) 36 (1991); *Phys. Rev. D* **24** 1516 (1981); *Phys. Rev. D* **26** 1862 (1982)
87. Gerry C, Hach E E *Phys. Lett. A* **174** 185 (1993)
88. Garraway B R, Knight V *Phys. Rev. A* **49** 1266 (1994); **50** 2548 (1994)
89. Filho M R L,Vogel W *Phys. Rev. Lett.* **76** 608 (1996)
90. Poyatos J F, Cirac J I, Zoller P *Phys. Rev. Lett.* **77** 4728 (1996)
91. Horoshko D B Kilin S Ya *Phys. Rev. Lett.* **78** 840 (1997)
92. Kilin S Ya, Horoshko D B, Shatokhin V N *Acta Phys. Pol. A* **93** 97 (1998)
93. Kilin S Ya, Horoshko D B *J. Mod. Opt.* **44** 2043 (1997); *Opt. Express* **2** 347 (1998)
94. Vitali D, Tombesi P, Milburn G J *Phys. Rev. Lett.* **79** 2442 (1997)
95. Zanardi P, Rasetti M *Phys. Rev. Lett.* **79** 3306 (1997)
96. Kilin S Ya, Shatokhin V N *Phys. Rev. Lett.* **76** 1051 (1996); *Zh. Eksp. Teor. Fiz.* **111** 1174 (1997) [*JETP* **84** 647 (1997)]; *Opt. Spektrosk.* **82** 972 (1997) [*Opt. Spectrosc.* **82** 893 (1997)]
97. Davies E B *Quantum Theory of Open Systems* (New York: Academic Press, 1976)
98. Kilin S Ya *Kvantovaya Optika, Polya i ikh Detektirovanie* (Quantum Optics, Fields and Their Detection) (Minsk: Navuka i Tehnika, 1990) [Translated into English (New York: Gordon Breach, 1988)]
99. Kholevo A S *Izv. Vyssh. Uchebn. Zaved. Matematika* **(8)** 3 (1982)
100. Quantum computations and cryptography in Los Alamos, http://qso.lanl.gov/qc/;
Quantum computations and cryptography in Oxford, http://eve.physics.ox.ac.uk/QChome.html;
Laboratory of theoretical and quantum computations, Montreal University,
http://www.iro.umontreal.ca/labs/theorique/index_en.html;
Quantum computations in IBM, http://www.research.ibm.com/xw-quantuminfo;
Introduction to quantum computations,
http://chemphys.weizmann.ac.il/˜schmuel/comp/comp.html;
Quantum computations in Australian National University, http://aerodec.anu.edu.au/ qc/index.html;
Quantum information, http://vesta.physics.ucla.edu/ smolin;
Archive on quantum computations, http://feynman.stanford.edu/qcomp/;
Preprints on quantum information in the archive of Los Alamos, http://xxx.lanl.gov/archive/quant-ph/;
Preprints on quantum information in the archive of ICTP, Trieste, http://www.ictp.trieste.it/indexes/preprints.html;
Quantum optics, http://master.bas-net.by/
101. Kadomtsev B B *Dinamika i Informatsiya* (Dynamics and Information) (Moscow: Uspekhi Fizicheskikh Nauk, 1997); 2nd ed. (Moscow: Uspekhi Fizicheskikh Nauk, 1999)