Physics – Uspekhi **48** (1) 1 – 36 (2005)

REVIEWS OF TOPICAL PROBLEMS PACS numbers: 03.65.Yz, **03.67.–a**, 03.67.Lx

Quantum computers and quantum computations

K A Valiev

DOI: 10.1070/PU2005v048n01ABEH002024

Contents

K A Valiev Institute of Physics and Technology,
Russian Academy of Sciences,
Nakhimovskiĭ prosp. 36/1, 117218 Moscow, Russian Federation
Tel. (7-095) 125 77 09. Fax (7-095) 129 31 41
E-mail: valiev@ftian.oivta.ru

Received 15 July 2004, revised 20 October 2004
Uspekhi Fizicheskikh Nauk **175** (1) 3 – 39 (2005)
Translated by E N Ragozin; edited by A M Semikhatov

Abstract. This review outlines the principles of operation of quantum computers and their elements. The theory of ideal computers that do not interact with the environment and are immune to quantum decohering processes is presented. Decohering processes in quantum computers are investigated. The review considers methods for correcting quantum computing errors arising from the decoherence of the state of the quantum computer, as well as possible methods for the suppression of the decohering processes. A brief enumeration of proposed quantum computer realizations concludes the review.

1. Introduction

1.1 Classical and quantum devices

The main technical accomplishments of the XXth century are inextricably entwined with the elucidation of the quantum laws of the structure of matter. Laser technology is based on the knowledge of quantum electronic spectra in gases, semiconductors, and dielectrics. The quantum theory of the band structure of electronic spectra in semiconductors underlies transistor physics. Nuclear power engineering relies on the understanding of the quantum laws of atomic nuclear structure.

Although the operation of lasers and transistors is based on the use of the quantum properties of matter, these devices nevertheless operate most often in the classical regime. Indeed, the electron currents and the voltages across transistor electrodes are classical quantities resulting from averaging over a large ensemble of particles. Similarly, coherent laser radiation is described by the laws of classical electrodynamics.

The classical character of laser radiation stems from the occurrence of a large ensemble of laser radiation photons. In going over to a single-photon regime (single-atom lasers), a laser becomes a quantum device in the sense that not only is its operation based on quantum laws, but also its radiation is a quantum object, for instance, a single photon. A transistor in a single-electron regime may become a quantum device if the electron dynamics is described by the quantum Schrödinger equation (the so-called ballistic transistor regime).

Therefore, one and the same device may operate both in the classical regime and in the quantum regime. The notions 'a classical device' and 'a device operating in the classical regime' are to be considered identical. The operation of a classical device is described by equations of classical physics with classical variables.

The term quantum device is to be used in reference to a device operating in the quantum regime. The quantum regime implies that the dynamics of the device are described by the Schrödinger equation for the wave function. The arguments of the wave function are quantum variables (coordinates, momenta, particle spins). The wave function of a quantum system has quantum coherence in the ordinary sense of the capacity to manifest interference effects on combining different components of the wave function. The coherence property of the wave function describing a quantum device is its most important distinguishing feature. We use the term 'quantum device' as a shortened version of the term 'quantum-coherent device'. [1]

To date, all devices employed in practical human activities have been classical. Nevertheless, the XXth century technical revolution in informatics and power engineering can justifiably be referred to as the first quantum revolution, so indissolubly related is it to quantum physics. Now let us imagine that we have overcome technological and other difficulties standing in the way of the advancement of quantum-coherent devices and have developed new-generation devices and technical systems that harness quantum technologies in practical activity. This would be the implementation of the second quantum revolution [1].

The laws of classical and quantum physics exhibit fundamental distinctions. Quantum-coherent devices and quantum technologies are therefore expected to be categorically different from classical devices and technologies of a similar purpose. It would be of practical significance should the dissimilarity between quantum devices and technologies and their classical analogs imply their 'advantages'. In other words, quantum engineering and technology should be an aid in overcoming the 'limits' and restrictions inherent in classical devices.

Theoretical analysis and experiments demonstrate that such potentialities do exist. It is possible, for instance, to overcome the diffraction resolution limit in quantum optical microscopy and quantum optical lithography [2] and to realize 'perfectly secure' quantum communication lines (quantum cryptography) [3]. In quantum metrology, it is possible to raise the sensitivity of interference devices by several orders of magnitude [2, 4]. For lack of space, these interesting topics remain outside the scope of our review, which is concerned with quantum computers and quantum computations performed with their aid. Quantum computers offer significant advantages over their classical counterparts and may furnish solutions to problems that are reputed to be insoluble with classical computers. The development of quantum computers involves overcoming both technological difficulties and the limitations arising from the decoherence of the states of a quantum computer. These problems are discussed in subsequent sections of this review.

The interest in experiments on quantum particle dynamics was rekindled in the last quarter of the XXth century due to the advent of radically new experimental techniques that make it possible to retain single atoms, ions, and electrons, cool them to ultralow temperatures (ranging down to nanokelvins), transfer them, and, most importantly, control their quantum dynamics. Techniques for confining charged particles in electromagnetic traps have enabled increasing their confinement time to many weeks, cooling the particles to ultralow temperatures by lasers, and investigating their spectra under extreme isolation conditions with the aim of developing frequency and time standards.

The states of substances termed one-dimensional ionic crystals have been realized in Paul traps [5]. Static and alternating external electric fields prevent the chain of ions in the trap from dispersing due to the Coulomb repulsion of the ions. The fields can be selected such that the equilibrium ion separation is equal to several micrometers, making it possible to separately act upon every ion with, for instance, a focused laser beam, to control the quantum evolution of the ion state. This structure is a popular model for experiments aimed at making one of the prototypes of a quantum computer [6]. In the construction of this model, advantage was taken of the progress in ultrahigh vacuum technology, original electric traps, laser cooling, and laser control of quantum dynamics.

A similar one-dimensional chain of phosphorus atoms ^{31}P can be embedded in the spinless dielectric crystal of ^{28}Si cooled to a temperature of the order of 1 mK [7]. The quantum dynamics of the nuclear and electron spins of the ^{31}P atoms can be controlled by pulsed nuclear and electronic magnetic resonance techniques. Selective access to an individual atom is achieved by tuning its resonance frequencies by way of control of the electronic structure of the atom

[1] This generates the necessity to clarify the content of the term 'quantum-electronics device'. This term is not equivalent to the term 'quantum device'. As shown above, a quantum-electronics device (a laser) may be a classical device (the classical regime) as well as a quantum device (the quantum-coherent regime). In modern optics, the description of quantum-coherent effects and devices is singled out as the area of 'quantum optics'.

through electric fields across nanoelectrodes. Constructing this structure calls for the development and use of the methods of so-called atomic scale resolution nanotechnology. Other proposals to make the elements of a quantum computer involving a solid rely on the physics of low-dimension electronic systems in semiconductors — two-dimensional electron gas, electrons in quantum wires, and quantum dots. These structures are fabricated by molecular epitaxy and nanolithography.

1.2 Algorithms: their complexity classes

To solve a problem, a computer, be it classical or quantum, performs a certain sequence of operations (instructions). The description of this sequence of operations is called an algorithm for the solution of the problem. The problem is characterized by its dimension n equal, for instance, to the number of binary digits in a number over which the algorithm is executed. The algorithm is realized by some operation circuit N_n, which depends on n; the circuit N_{n+1} is obtained from N_n by simple rules.

In the algorithm complexity theory for classical computers, the practice is to divide algorithms into the categories of efficient and inefficient. An algorithm belongs to the class of efficient ones if the circuit N_n consists of a polynomial number of operations $O(n^d)$, where $d = \text{const}$ and n is the dimension of the problem. The time required for the execution of an efficient algorithm increases polynomially with the dimension of the problem: $t_n \propto n^d$. In this instance, the resource utilized for solving the problem is the computer operation time. Among other resources are the computer memory capacity and (for a quantum computer) the accuracy of operation execution. An efficient algorithm should utilize a polynomial amount of resources that are limited. Efficient algorithms are also termed polynomial (P class).

Efficient P-class algorithms can be contrasted with inefficient ones, which require exponentially large resources (of time, memory, and accuracy). For instance, if $t_n \propto 2^n$, the algorithm is classed with inefficient ones. An example of a problem for which no efficient algorithm for solving with a classical computer has been found is the task of calculating prime factors for large n-digit numbers (the task of number factorization).[2] The best-known probabilistic algorithm for classical computers requires $2^{\alpha(n\log_2 n)^{1/2}}$ operations [8].

In 1994, Shor constructed an algorithm for the solution of this problem with a quantum computer, which turned out to be of polynomial complexity: the requisite number of operations is $O\big(n^2 \log_2 (\log_2 n \log_2 \varepsilon^{-1})\big)$, where ε is the error per single computational operation [9]. Shor's result was a sensation. It refuted the so-called Church–Turing thesis (empirical law), which states that all computers are equivalent in the sense that changing from one computer to another does not change the task complexity class. The thesis was formulated for the ensemble of classical computers; the thesis is broken when the ensemble comprises quantum computers.

This result came as no surprise to physicists. Information is not a purely mathematical concept. It has a physical carrier: it is coded, stored, processed, transmitted, written, and erased by changing the state of the information carrier. Information is physical [10]. The existence of an intimate linkage between physics and information comes to light when the thermodynamic entropy in physics is compared with Shannon's information entropy in information theory: they coincide up to a constant factor.

The fundamental differences between classical and quantum laws of physics underlie the fundamental differences between classical and quantum information as well as between the methods for processing them. The physical information theory comprises the classical and quantum information theories, and in a broader sense (with the introduction of the corresponding technical means into the concept) comprises classical and quantum informatics. Among the remarkable achievements of classical information theory is the solution of the paradox of the Maxwell demon, which violates the second law of thermodynamics. The paradox vanishes when one takes the properties of information erasing into account [10]: erasing 1 information bit is accompanied by the expenditure of the energy $kT\ln 2$ and an increase in entropy by $k\ln 2$ (Landauer's principle, 1961).

2. Qubits: properties and mathematical description of states

2.1 Bits and qubits

The terms 'bit' and 'qubit' denote the units of classical and quantum information, as well as classical and quantum systems, that are carriers of 1 information bit (qubit).

In modern classical computers, there are memory bits, which store information, and controllable bits in 'circuits', which process information. In the magnetic memory of a computer, a bit is a magnetized region of a magnetic film: to two magnetization directions there correspond the '0' and '1' values of the information bit. The switching '0' → '1' or '1' → '0' requires overcoming the energy barrier between the two states of the film; it is the existence of the barrier that ensures the reliability of information storage.

In the random-access memory of a computer, the information carrier is a trigger transistor circuit. In the memory cells described above, the states '0' and '1' are separated by an energy barrier. Moreover, states with minimal energy are attractors to which the system evolves from the set of states surrounding an attractor. The reliability of information storage in classical computers is ensured by the existence of the energy barrier that separates the two attractors representing the states '0' and '1'.

An example of a controllable bit employed in information processing systems in computers (processors) is provided by an inverter built around two transistors (Fig. 1). In the inverter, the input voltage V_{in} 'controls' the voltage V_{out} at

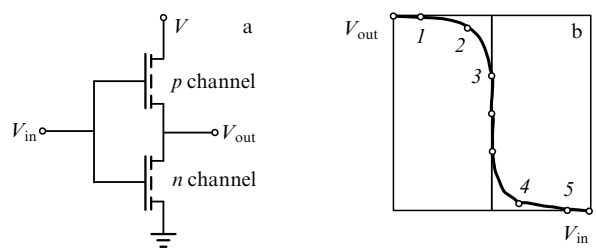

Figure 1. Classical inverter circuit involving two field transistors (a) and the transfer function of the inverter (b). The states '0' and '1' at the input (V_{in}) and output (V_{out}) are coded with the values of electric voltage.

[2] The proof that an efficient algorithm for the solution of this problem is nonexistent has not been found.

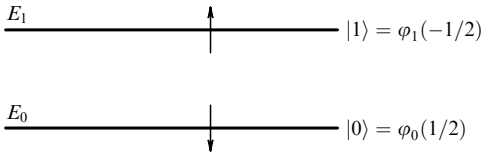

Figure 2. Schematic of a quantum bit — a qubit. The logical qubit states $|0\rangle$ and $|1\rangle$ correspond to the energy eigenfunctions of the spin $I = 1/2$ or the projection I_z in a constant magnetic field B.

the output: if V_{in} corresponds to the value '0' ('1'), V_{out} corresponds to '1' ('0'). The inverter performs the logical NOT operation. In this case, use is made of the nonlinear functional relation

$$V_{\text{out}} = f(V_{\text{in}}),$$

which is defined by transistor properties and their coupling in the system.

The basis element of a quantum computer (the carrier of quantum information) is a quantum bit — a qubit. In quantum communication systems, information is transmitted by the physical transfer of a qubit — the information carrier — or by teleportation of the quantum state of the qubit.

For a qubit, one can select any quantum system with two states characterized by orthonormal wave functions $|\varphi_0\rangle$ and $|\varphi_1\rangle$. A convenient example of a qubit is the nuclear (or electron) spin $I = 1/2$, with two energy levels in a constant external magnetic field B,

$$E_0 = -\frac{1}{2}\hbar\gamma B, \qquad E_1 = \frac{1}{2}\hbar\gamma B,$$

corresponding to the spin directions along the field or opposite to it (Fig. 2). The wave functions

$$|\varphi_0\rangle = \left|I_z = \frac{1}{2}\right\rangle, \qquad |\varphi_1\rangle = \left|I_z = -\frac{1}{2}\right\rangle$$

are the eigenfunctions of the operator of the total spin energy in the magnetic field B:

$$H = -I_z\hbar\gamma B.$$

Another example of a qubit is the Ca^{2+} ion as a part of a one-dimensional ionic crystal. The energy level diagram of the Ca^{2+} ion is given in Fig. 3. The $4\,^2S_{1/2}$ sublevel can be selected for the $|0\rangle$ qubit state and the $3\,^2D_{5/2}$ sublevel of the excited metastable ion state for $|1\rangle$. Electric dipole transitions between the S and D levels are forbidden and electric quadrupole transitions are allowed, such that the lifetime of the Ca^{2+} ion in the D state amounts to 1 s.

Attention is drawn to the fact that there is no energy barrier between the $|0\rangle$ and $|1\rangle$ qubit states: the $|1\rangle$ state is unstable with respect to transition to the $|0\rangle$ state. Other Ca^{2+} ion states (except for the qubit states) are auxiliary in the organization of qubit dynamics, for instance, in the cooling of the qubit and the measurement of its state [5]. The $4\,^2S_{1/2} \leftrightarrow 3\,^2D_{5/2}$ transitions (the qubit dynamics) are controlled by laser pulses at the transition frequency. The laser beam is focused on a single ion in the ion crystal [5].

There are also other versions for selecting the qubit states. When the ground state of an ion is degenerate with respect to spin $S = 1/2$, it splits into two spin sublevels $|\pm 1/2\rangle$ in a

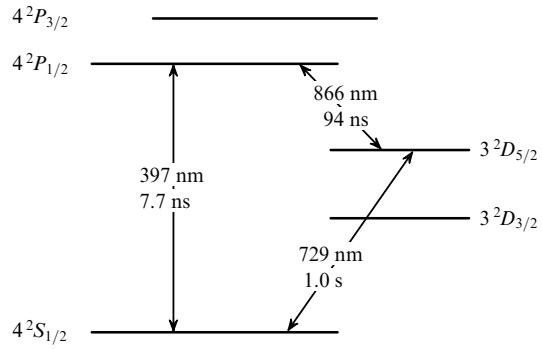

Figure 3. Schematic of a qubit in the system of energy eigenvalues and eigenfunctions of the Ca^{2+} ion. The states $|4\,^2S_{1/2}\rangle = |0\rangle$ and $|3\,^2D_{5/2}\rangle = |1\rangle$ are selected as the qubit states. The $|1\rangle \to |0\rangle$ spontaneous decay proceeds slowly (in 1 s).

constant magnetic field B, and these can be adopted as the $|0\rangle$ and $|1\rangle$ qubit states. The $|+1/2\rangle \leftrightarrow |-1/2\rangle$ transitions can be controlled by the combined action of the fields of two lasers tuned to operate by the so-called Raman scheme. The laser frequency difference in the Raman scheme is equal to the frequency of the transition between the $|\pm 1/2\rangle$ sublevels: the higher-frequency photon (of the pump laser) is absorbed in the transition from the $|0\rangle$ level to an intermediate virtual energy level near an auxiliary level $|2\rangle$, and at the lower frequency of the Stokes laser, there occurs stimulated emission of a photon in the transition from the virtual level to the $|1\rangle$ level.

Orbital electron states in quantum wells or quantum dots are selected for qubit states in other popular realizations. The '0' and '1' electron states in quantum dots may be selected by a potential barrier, as in the realization of a classical bit. Nevertheless, in the quantum case, the '1' state remains unstable with respect to the '1' → '0' decay due to the possibility of a tunnel transition through the barrier. Laser pulses control the qubit dynamics via excited electron energy levels [11].

Considerable interest is attracted to qubit realizations involving superconducting structures. In a charge superconducting qubit, the $|0\rangle$ and $|1\rangle$ states correspond to the absence and presence of the charge of a single Cooper pair in a metallic superconducting quantum dot [12]. The $|0\rangle$ and $|1\rangle$ qubit states in a SQUID (a superconducting ring with Josephson junctions in a magnetic field) correspond to oppositely directed superconducting currents [13].

A large number of experiments have been performed on a single-photon qubit. Any two photon states with orthogonal polarizations may be selected as the $|0\rangle$ and $|1\rangle$ qubit states. The adoption of two photon states that differ by π in phase is also possible. Systems of photon and atomic qubits in a resonator make up the basis system for experiments in the branch of quantum optics called cavity quantum electrodynamics (cavity QED) [14].

2.2 A qubit in the Hilbert vector space of states

In the foregoing, we adduced examples of two orthonormal states of different quantum systems selected as the basis $|0\rangle$ and $|1\rangle$ qubit states. Any qubit state $|\varphi\rangle$ normalized to unity can be expanded in terms of this basis:

$$|\varphi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1. \tag{1}$$

State (1) expresses the superposition principle of quantum mechanics as a linear theory: if the states $|0\rangle$ and $|1\rangle$ are solutions of the Schrödinger equation for the system, any superposition of these solutions is also a solution of the equation.

The set of state vectors $|\varphi\rangle$ makes up the two-dimensional Hilbert vector space of a qubit. The components of two-dimensional vectors $|0\rangle$, $|1\rangle$, and $|\psi\rangle$ are written in the form of columns:

$$|0\rangle = \begin{vmatrix} 1 \\ 0 \end{vmatrix}, \quad |1\rangle = \begin{vmatrix} 0 \\ 1 \end{vmatrix}, \quad |\psi\rangle = a\begin{vmatrix} 1 \\ 0 \end{vmatrix} + b\begin{vmatrix} 0 \\ 1 \end{vmatrix} = \begin{vmatrix} a \\ b \end{vmatrix}. \quad (2)$$

The states $|0\rangle$ and $|1\rangle$ are basis vectors in the two-dimensional Hilbert space of the qubit. The $|\psi\rangle$ projections on the basis vectors are equal to the amplitudes a and b in the superposition:

$$\langle 0|\psi\rangle = a\,, \quad \langle 1|\psi\rangle = b\,.$$

Generally, the amplitudes a and b are some complex numbers:

$$a = |a| \exp(\mathrm{i}\varphi_a)\,, \quad b = |b| \exp(\mathrm{i}\varphi_b)\,.$$

Then,

$$|\psi\rangle = \exp(\mathrm{i}\varphi_a)\big[|a| + |b| \exp\big(\mathrm{i}(\varphi_b - \varphi_a)\big)\big]\,.$$

The common phase factor $\exp(\mathrm{i}\varphi_a)$ has no effect on the results of qubit state measurements, and the phase φ_a may have an arbitrary value. Hence, it follows that the $|\psi\rangle$ vector is defined by two real parameters, for instance $|a|$ and $(\varphi_b - \varphi_a)$. The values of $|a|^2$ and $|b|^2 = 1 - |a|^2$ are determined by multiple measurements, in the basis $|0\rangle$, $|1\rangle$, over the qubit ensemble prepared in the $|\psi\rangle$ state, and are defined as the probabilities of the measurement results:

$$p\big(|0\rangle\big) = |a|^2\,, \quad p\big(|1\rangle\big) = |b|^2\,.$$

The phase difference $(\varphi_b - \varphi_a)$ of the amplitudes may be determined from interference-type experiments (see below).

The transformations of the vector

$$|\psi\rangle = \begin{vmatrix} a \\ b \end{vmatrix}$$

to the vector

$$|\psi'\rangle = \begin{vmatrix} a' \\ b' \end{vmatrix}$$

are single-qubit quantum operations in quantum computations. Geometrically, this transformation is the rotation of the vector

$$|\psi\rangle = \begin{vmatrix} a \\ b \end{vmatrix}$$

until it coincides with the vector

$$|\psi'\rangle = \begin{vmatrix} a' \\ b' \end{vmatrix}.$$

The rotation operator U is a unitary 2×2 matrix,

$$\begin{vmatrix} a' \\ b' \end{vmatrix} = \mathrm{U}(2 \times 2)\begin{vmatrix} a \\ b \end{vmatrix}.$$

From the general form of the matrix

$$\mathrm{U} = \begin{pmatrix} c\exp(-\mathrm{i}\alpha) & -t\exp(\mathrm{i}\beta) \\ t\exp(-\mathrm{i}\beta) & c\exp(\mathrm{i}\alpha) \end{pmatrix},$$

where c, t, α, and β are real numbers, we conclude that it is unitary if $c^2 + t^2 = 1$.

The rotation of a vector in the Hilbert space is continuous: in its rotation by a finite angle, the vector $|\psi\rangle$ goes through a continuous sequence of intermediate orientations. The matrix of rotation by a finite angle is an ordered product of the matrices of rotation by infinitesimal angles [15]. The continuity of transitions is the distinctive feature of quantum mechanics, which underlies its axiomatic formulation [16].

A qubit 'exists' simultaneously in the abstract two-dimensional Hilbert space and in the three-dimensional Euclidean space. (A similar statement applies to a quantum computer as an ensemble of qubits.) Computational operations are performed in the Hilbert space as the transformations of the state vector:

$$|\psi'\rangle = \mathrm{U}(2 \times 2)\,|\psi\rangle\,.$$

The physical processes in the quantum system selected for the qubit must be simultaneously described in the three-dimensional Euclidean space. In the laboratory frame of reference $Oxyz$, we should be able to perform physical operations that result in the desired transformation U of the qubit state vector in the Hilbert space. This task is solved by the following theorem [15].

The matrix of an arbitrary unitary qubit transformation U in the Hilbert space can be represented as a product of three matrices describing the rotation of the state vector,

$$\mathrm{U} = \exp(\mathrm{i}\alpha)\,\mathrm{R}_{\mathbf{n}}(\beta)\,\mathrm{R}_{\mathbf{m}}(\gamma)\,\mathrm{R}_{\mathbf{n}}(\delta)\,,$$

where $\mathbf{n}$ and $\mathbf{m}$ are two nonparallel unit vectors in the system of coordinates $Oxyz$ and $\mathrm{R}_{\mathbf{n}}(\theta)$ is the matrix (operator) of rotation about the axis $\mathbf{n}$ by an angle θ.

In the context of a real experiment, the n- and m-axes are conveniently superposed on the axes of the system of coordinates $Oxyz$. Then zy- and xy-expansions are possible [15]:

$$\begin{aligned} \mathrm{U} &= \exp(\mathrm{i}\alpha)\,\mathrm{R}_z(\beta)\,\mathrm{R}_y(\gamma)\,\mathrm{R}_z(\delta) \quad (zy\text{-expansion})\,, \\ \mathrm{U} &= \exp(\mathrm{i}\alpha)\,\mathrm{R}_x(\beta)\,\mathrm{R}_y(\gamma)\,\mathrm{R}_x(\delta) \quad (xy\text{-expansion})\,. \end{aligned} \quad (3)$$

The matrices of rotation about the x, y, and z axes have the form [15]

$$\begin{aligned} \mathrm{R}_x(\varphi) &= \begin{pmatrix} c & -\mathrm{i}s \\ -\mathrm{i}s & c \end{pmatrix}, \\ \mathrm{R}_y(\varphi) &= \begin{pmatrix} c & -s \\ s & c \end{pmatrix}, \\ \mathrm{R}_z(\varphi) &= \begin{pmatrix} c + \mathrm{i}s & 0 \\ 0 & c - \mathrm{i}s \end{pmatrix}, \end{aligned} \quad (4)$$

where $c = \cos(\varphi/2)$ and $s = \sin(\varphi/2)$. We substitute the rotation matrices R_z, R_y into the zy-expansion and multiply the matrices to obtain

$$U = \exp(i\alpha) \times \begin{pmatrix} \cos\frac{\gamma}{2}\exp\left(-i\,\frac{\beta+\delta}{2}\right) & -\sin\frac{\gamma}{2}\exp\left(-i\,\frac{\beta-\delta}{2}\right) \\ \sin\frac{\gamma}{2}\exp\left(i\,\frac{\beta-\delta}{2}\right) & \cos\frac{\gamma}{2}\exp\left(i\,\frac{\beta+\delta}{2}\right) \end{pmatrix}. \quad (5)$$

In the Hilbert space, we specify the transformation U by the matrix

$$U = \exp(i\alpha)\begin{pmatrix} a\exp(-iu) & -b\exp(iv) \\ b\exp(-iv) & a\exp(iu) \end{pmatrix} \quad (6)$$

and require that matrices (5) and (6) be identical, and then

$$a = \cos\frac{\gamma}{2}, \quad b = \sin\frac{\gamma}{2}, \quad \delta = \frac{u+v}{2}, \quad \beta = \frac{u-v}{2}. \quad (7)$$

Therefore, an arbitrary transformation of the qubit state vector with parameters according to expression (6) may be executed as successive rotations of this vector about the z, y, and z axes of the laboratory system of coordinates by the angles δ, γ, and β according to expression (7).

The rotations $R_x(\theta)$, $R_y(\theta)$, and $R_z(\theta)$ of the qubit state vector $|\varphi\rangle$ are considered elementary single-qubit computational operations. They should be related to the parameters of the physical fields that control the dynamics of the quantum system selected as the qubit. For instance, in the case of the $I = 1/2$ spin qubit, the rotation of its state vector in the magnetic field

$$\mathbf{B} = B_0\mathbf{z} + B_1\mathbf{x}\cos(\omega t)$$

(where $\gamma B_0 \equiv \omega_0$ and $\gamma B_1 = \Omega$) is described by the equation [15]

$$|\varphi(t)\rangle = \exp\left[i\left(\frac{\omega-\omega_0}{2}Z + \Omega X\right)t\right]|\varphi(0)\rangle. \quad (8)$$

Here, Z and X are the Pauli matrices and $\mathbf{z}$ and $\mathbf{x}$ are the unit vectors along the z and x axes of the system of coordinates $Oxyz$.

Equation (8) corresponds to the rotation of $|\varphi\rangle$ about the axis

$$\mathbf{n} = \frac{\mathbf{z} + \lambda\mathbf{x}}{(1+\lambda^2)^{1/2}}$$

by the angle

$$\theta = \Omega t\left(1 + \frac{1}{\lambda^2}\right)^{1/2}, \quad \lambda = \frac{2\Omega}{\omega_0 - \omega}.$$

Exactly at resonance ($\omega = \omega_0$), the axis of rotation $\mathbf{n}$ of the vector $|\varphi\rangle$ coincides with the $\mathbf{x}$ axis and the angular velocity of rotation with the so-called Rabi frequency Ω (see Section 3.6):

$$\mathbf{n} = \mathbf{x}, \quad \theta = \Omega t.$$

For routine single-qubit operations in quantum computations, use is quite often made of state-vector transformations expressed in terms of the Pauli matrices:

$$R_x(\pi) \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad R_y(\pi) \equiv Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad R_z(\pi) \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (9)$$

The matrix of the transformation involving a phase change of the state vector (a phase gate) is of the form

$$U(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\varphi) \end{pmatrix}, \quad (10)$$

and the Hadamard transformation matrix is

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(X + Z). \quad (11)$$

It is easily verified that

$$X\begin{vmatrix} a \\ b \end{vmatrix} = \begin{vmatrix} b \\ a \end{vmatrix} = \mathrm{NOT}\begin{vmatrix} a \\ b \end{vmatrix}, \quad Z\begin{vmatrix} a \\ b \end{vmatrix} = \begin{vmatrix} a \\ -b \end{vmatrix},$$

$$U(\varphi)\begin{vmatrix} a \\ b \end{vmatrix} = \begin{vmatrix} a \\ b\exp(i\varphi) \end{vmatrix},$$

$$H|0\rangle = H\begin{vmatrix} 1 \\ 0 \end{vmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

$$H|1\rangle = H\begin{vmatrix} 0 \\ 1 \end{vmatrix} = \frac{1}{2}\left(|0\rangle - |1\rangle\right).$$

Up to a common phase factor, $X = \mathrm{NOT} = R_x(\pi)$: the NOT negation operation is executed by the rotation of the qubit state vector about the x axis by the angle π.

We also give the definition of the scalar product of the vectors $|\varphi_i\rangle = a_i|0\rangle + b_i|1\rangle$ and $|\varphi_j\rangle = a_j|0\rangle + b_j|1\rangle$:

$$\langle\varphi_j|\varphi_i\rangle = a_j^* a_i + b_j^* b_i.$$

Geometrically, it defines the 'angle' θ between the vectors:

$$\cos\theta = \langle\varphi_j|\varphi_i\rangle.$$

The state of the qubit $|\varphi\rangle = a|0\rangle + b|1\rangle$ can be mapped onto a point on the surface of the three-dimensional unit Bloch sphere in Euclidean space. The spherical coordinates θ and φ of a point on the surface of the sphere are related to the amplitudes a and b by

$$\cos\frac{\theta}{2} = a, \quad \exp(i\varphi)\sin\frac{\theta}{2} = b$$

(the amplitude a can be treated as a real number owing to the unobservability of the common phase). This bijective correspondence implies the isomorphism of rotation groups in the two-dimensional Hilbert space and the three-dimensional Euclidean space:

$$SU(2) \simeq SO(3).$$

2.3 Quantum coherence of state vectors

The states of a quantum system described by the vectors of state $|\psi\rangle$ are called pure. Pure and mixed states of quantum

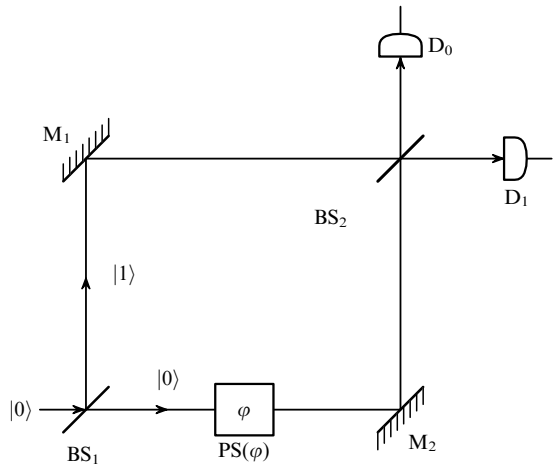

Figure 4. Schematic of photon interference in the Mach–Zehnder interferometer: BS_1, BS_2 — 50/50 beamsplitters; M_1, M_2 — mirrors; $PS(\varphi)$ — phase shifter; D_1, D_2 — single-photon detectors. Interference reveals the quantum coherence of the photon state.

systems are fundamentally different on the basis of coherence: the pure states are coherent and the mixed states are incoherent.

The concept of coherence in quantum physics is defined similarly to the concept of coherence in optics: the wave functions (state vectors) of quantum-coherent systems have the interference capability. The famous experiment in the observation of electron diffraction from two slits is actually an experiment in the revelation of the quantum coherence of the orbital wave function $|\psi(r)\rangle$ of a free electron. We demonstrate the coherence of the wave function of a single photon with a Mach–Zehnder interferometer [14]. The interferometer is schematically shown in Fig. 4.

The wave function of a photon incident on a beamsplitter BS_1 horizontally (vertically) is assumed to be the basis state $|0\rangle$ ($|1\rangle$). The 50/50 beamsplitter reflects or transmits photons with equal amplitudes $1/\sqrt{2}$. In the interferometer, the reflected and transmitted photons are permitted to propagate along different paths, i.e., the photon acquires a new degree of freedom.

We introduce new basis photon states $|0\rangle$ and $|1\rangle$ corresponding to the motion along two possible paths. With the $\pi/2$ phase difference between the reflected and transmitted waves, the beamsplitter BS_1 performs the transformations of the states $|0\rangle$ and $|1\rangle$ at the beamsplitter input

$$|0\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\,, \qquad |1\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\,, \tag{12}$$

which are equivalent to the Hadamard transformation

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

We consider the interference in a Mach–Zehnder interferometer for an incoming photon in the $|0\rangle$ state:

$$|0\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \xrightarrow{PS(\varphi)} \frac{1}{\sqrt{2}}\big(|0\rangle \exp(\mathrm{i}\varphi) + |1\rangle\big)$$
$$= \frac{1}{\sqrt{2}} \exp\frac{\mathrm{i}\varphi}{2}\left[|0\rangle \exp\frac{\mathrm{i}\varphi}{2} + |1\rangle \exp\left(-\frac{\mathrm{i}\varphi}{2}\right)\right]. \tag{13}$$

A beamsplitter BS_2 subjects the states $|0\rangle$ and $|1\rangle$ in expression (13) to the Hadamard transformation again. As a result, we obtain the photon wave function at the output of the beamsplitter BS_2:

$$\frac{1}{2}\exp\frac{\mathrm{i}\varphi}{2}\left[\exp\frac{\mathrm{i}\varphi}{2}\big(|0\rangle + |1\rangle\big) + \exp\left(-\frac{\mathrm{i}\varphi}{2}\right)\big(|0\rangle - |1\rangle\big)\right]$$
$$= \exp\frac{\mathrm{i}\varphi}{2}\left[|0\rangle\cos\frac{\varphi}{2} + |1\rangle \mathrm{i}\sin\frac{\varphi}{2}\right]. \tag{14}$$

The interference of the coherent wave functions transmitted by the two interferometer arms determines the photon detection probabilities at the detectors:

$$p_0 = \cos^2\frac{\varphi}{2} = \frac{1+\cos\varphi}{2}\,, \qquad p_1 = \sin^2\frac{\varphi}{2} = \frac{1-\cos\varphi}{2}\,. \tag{15}$$

The interference of state amplitudes is a typical process in quantum computations. We demonstrate it by the example of a simple computation with two qubits in the initial state $|00\rangle$ (the first and second zeroes correspond to the states of the first and second qubits). The computations consist in the $H_1H_2H_1NOT_1$ operation sequence:

$$|00\rangle \xrightarrow{NOT_1} |10\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\big(|0_1\rangle - |1_1\rangle\big)|0_2\rangle$$
$$\xrightarrow{H_2} \frac{1}{2}\big(|0_1\rangle - |1_1\rangle\big)\big(|0_2\rangle + |1_2\rangle\big)$$
$$\xrightarrow{H_1} \frac{1}{2\sqrt{2}}\big[|00\rangle(1-1) + |10\rangle(1+1)$$
$$+ |01\rangle(-1+1) + |11\rangle(1+1)\big]. \tag{16}$$

The sums of the amplitudes in the $|00\rangle$ and $|01\rangle$ states are zero because the amplitudes interfere destructively, while the interference of the amplitudes in the $|10\rangle$ and $|11\rangle$ states is constructive.

3. Principles of design and operation of an ideal quantum computer

3.1 An ideal quantum computer

A quantum computer is diagrammed in Fig. 5. The quantum computer is actually a register of n qubits controlled by external (classical) signals. The quantum computer is embedded in a classical environment, which consists of a controlling classical computer and a pulse generator, which control the evolution of the qubits, as well as the devices for measuring the qubit states. Other registers (ancillas), which play an auxiliary role, may be added to the register n in the course of computations.

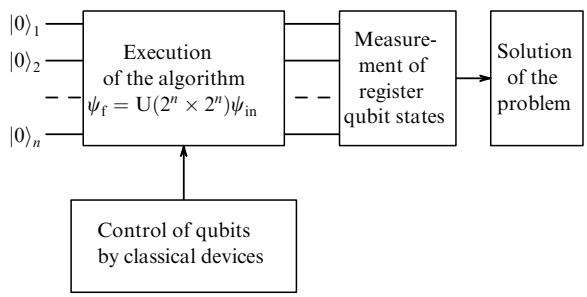

Figure 5. Schematic of a quantum computer.

A quantum computer whose states are always coherent is termed ideal. This implies, first, that the computer does not interact with an environment that produces noise and disturbs the coherence of the computer state vector (decohering action); second, external signals execute accurate control in an ideal computer.

The state vector $|\psi\rangle$ of the quantum register of n qubits is decomposed with respect to 2^n basis states of the register $|i_1 \dots i_n\rangle$, $i_1, \dots, i_n = \{0, 1\}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} |i_1 \dots i_n\rangle \,. \tag{17}$$

Here, the superposition $|\psi\rangle$ is a vector in the 2^n-dimensional vector space, $|i_1 \dots i_n\rangle$ are the 2^n basis vectors (unit vectors) of this space, and $a_{i_1,\dots,i_n}$ are the projections of the vector $|\psi\rangle$ on the directions of the unit vectors $|i_1 \dots i_n\rangle$. Everything that can be known about the physical system is contained in its state vector $|\psi\rangle$. All that can be done with the system is to transform its initial state vector $|\psi_{\rm in}\rangle$ to another vector $|\psi_{\rm f}\rangle$. That is why the process of computation by a quantum computer is considered as the transformation of the initial computer state vector $|\psi_{\rm in}\rangle$ to the final state vector $|\psi_{\rm f}\rangle$ by multiplying the $|\psi_{\rm in}\rangle$ vector by the unitary matrix U of size $2^n \times 2^n$:

$$|\psi_{\rm f}\rangle = {\rm U}(2^n \times 2^n)\, |\psi_{\rm in}\rangle \,. \tag{18}$$

It is conveniently assumed that all qubits reside in the state $|0\rangle$ in the initial state of the computer:

$$|\psi_{\rm in}\rangle = |0_1 \dots 0_n\rangle \,.$$

This operation is termed initialization. The state $|0_1 \dots 0_n\rangle$ can be obtained by cooling qubits to ultralow temperatures or by measuring and controlling the qubit states. The algorithm for problem solving is embodied in the transformation matrix ${\rm U}(2^n \times 2^n)$. Classical information on problem solving is embodied in the final state vector $|\psi_{\rm f}\rangle$; it should be obtained by measuring the qubits.

Solving a problem with a quantum computer requires making the necessary quantity of qubits, initializing them, controlling their quantum evolution, effecting the transformation ${\rm U}|\psi_{\rm in}\rangle$, and measuring the qubit states described by the vector $|\psi_{\rm f}\rangle = {\rm U}|\psi_{\rm in}\rangle$. We address this later and now consider the issue of the resources of a quantum computer that offer advantages over a classical computer.

We analyze the resource of a quantum computer on the basis of Eqn (18) of computer operation. We first introduce a more economical notation for the state vector $|\psi\rangle$. The basis state $|i_1 \dots i_n\rangle$ is an n-digit binary number $|x\rangle$ whose digits coincide with the numbers $i_1, \dots, i_n = \{0, 1\}$. In this notation,

$$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x |x\rangle \,.$$

The superposition $|\psi\rangle$ contains 2^n terms, which are the decomposition of the $|\psi\rangle$ vector in terms of the basis functions $|x\rangle$, $0 \leqslant x \leqslant 2^n - 1$. A limited physical resource, i.e., a small number $n \simeq 10^3$ of particles (qubits) creates an exponentially large $2^n = 2^{1000} \simeq 10^{300}$ mathematical informational resource in a quantum computer. The major advantages of the quantum computer stem precisely from this circumstance.

A consequence of the superposition principle is the 2^n-fold quantum parallelism of computations. Indeed, changing the state of only one qubit rearranges the entire superposition. (Because the set of basis functions $|x\rangle$ is constant, all the 2^n projections a_x of the vector $|\psi\rangle$ are rearranged.)

We compare these facts with the potentialities of the register of a classical computer. The classical register of n bits may reside in only one of 2^n states, because it does not obey the superposition principle. The classical register state is one-dimensional. Changing the state of one bit transfers the register to another one-dimensional state (close in value). The resources of a classical computer are exponentially small in comparison with those of a quantum computer. The Hilbert space of the states $|\psi\rangle$ is the state of complex numbers. This implies that the amplitudes a_x in the decomposition $|\psi\rangle = \sum a_x |x\rangle$ are complex numbers:

$$a_x = |a_x| \exp({\rm i}\varphi_x) \,.$$

In the addition of the vectors

$$|\psi\rangle + |\psi'\rangle = \sum (a_x + a'_x)\, |x\rangle$$

there occurs interference of quantum amplitudes, which we demonstrated by the example of a Mach – Zehnder interferometer for one qubit:

$$a_x + a'_x = \big[\big(|a_x| + |a'_x|\big) \cos\varphi_x^- + {\rm i}\big(|a_x| - |a'_x|\big) \sin\varphi_x^-\big] \exp({\rm i}\varphi_x^+) \,, \tag{19}$$

$$\varphi_x^{\pm} = \frac{\varphi_x \pm \varphi'_x}{2} \,.$$

In the course of quantum computation, the amplitude interference takes place everywhere and automatically. That is why some authors perceive a quantum computer as a sophisticated interferometer for the amplitudes of the state vector of the quantum computer.

This brings up the question: Is there a way to harness the effect of electromagnetic wave interference for effecting quantum computation? In other words, are optical computers the analogs of quantum computers? We compare the optical wave superposition with the superposition of state vectors in the quantum computer:

$$\sum_{j=1}^{l} E_j = \sum_{j=1}^{l} a_j \sin(\omega t + \varphi_j) \,, \tag{20}$$

$$\sum_{j=1}^{l} |\psi_j\rangle = \sum_{j=1}^{l} \sum_{x=0}^{2^n-1} a_x^{(j)} |x\rangle = \sum_{x=0}^{2^n-1} \Big(\sum_{j=1}^{l} a_x^{(j)} \Big) |x\rangle \,. \tag{21}$$

In an optical computer, there occurs a one-fold interference of the optical modes E_j; in a quantum computer, there occurs a 2^n-fold interference of the amplitudes for every vector $|x\rangle$, $0 \leqslant x \leqslant 2^n - 1$. The state vector of a quantum computer contains both digital ($|x\rangle$) and analog (a_x) information; an optical computer contains only analog (E_j) information. An optical computer cannot model quantum computations: it should be classified with classical analog computers.

3.2 The quantum computer — an analog-controlled digital computer

Analyzing the equation $|\psi_{\rm f}\rangle = {\rm U}|\psi_{\rm in}\rangle$ for a quantum computer allows one to determine the principle of operation and

control of the quantum computer. The state $|\psi_{\rm in}\rangle = |0_1 \ldots 0_n\rangle$ contains no information of either the problem or the methods of its solution. All the information about the problem to be solved and the algorithm for its solution is carried by the transformation matrix U. Lastly, the final state vector

$$|\psi_{\rm f}\rangle = \sum_{x=0}^{2^n-1} a_x^{(\rm f)} |x\rangle$$

contains the information about the solution of the problem. This information can be gained by measuring the state of each of n computer qubits in the state $|\psi_{\rm f}\rangle$, using the basis $|0\rangle$, $|1\rangle$ for measuring. Upon measuring, we obtain any of the values $0 \leqslant x \leqslant 2^n - 1$ with the probabilities $|a_x^{(\rm f)}|^2$, as is evident from the general principles of quantum physics.

How can different numbers x represent the solution of a problem when the solution has to be unique? This is so, indeed; only one value $|s\rangle$ is the solution, the remaining values $|x\rangle \neq |s\rangle$ are erroneous. For the idea of a quantum computer to be of physical significance, the quantum algorithm should lead to a state $|\psi_{\rm f}\rangle$ such that the probability of finding the correct solution is $p_s = |a_s|^2 \simeq 1$, while the sum of the probabilities of all erroneous solutions is small:

$$\sum_{x \neq s} |a_x|^2 \ll 1 \,.$$

All quantum algorithms invented to date have this property. Therefore, a quantum computer yields a digital solution of the problem s with a certain probability, i.e., is a digital probabilistic computer.

We now reveal the method of controlling a quantum computer. In the course of quantum computation, the initial state vector $|\psi_{\rm in}\rangle = \sum_x a_x^{(\rm in)} |x\rangle$ is transformed into the final vector $|\psi_{\rm f}\rangle = \sum_x a_x^{(\rm f)} |x\rangle$ via a continuous sequence of states. The basis set of states $|x\rangle$ remains invariable. The dynamics of the state of the computer are reflected in the time dependence of the amplitudes $a_x(t)$, which constitute analog quantities taking a continuous sequence of values in the interval $0 \leqslant |a_x| \leqslant 1$. To control the computer means controlling the $a_x(t)$ processes, i.e., a quantum computer is an analog computer with regard to the means of control.

This combination of properties — an analog means of control and the probabilistic nature of presentation of the digital solution — is inherent in none of the classical computer types. A quantum computer looks like a Minotaur in the realm of computers, combining the properties of analog and digital computers incompatible in the classical realm.

At the dawn of computer engineering (1950–1960), analog (classical) computers successfully complemented digital computers. More recently, they were displaced by digital computers owing to the low precision of resultant solutions. It was possible to monitor analog variables (currents and voltages) with an accuracy of the order 10^{-2}. According to modern estimates, the parameters of qubit-controlling signals (pulses) are to be controlled with an accuracy of 10^{-5}–10^{-4}. Hence, the price the originators of quantum computers will have to pay is high for the privilege of meeting the Minotaur — an analog-controlled digital computer. As shown below, a high accuracy of operations is required to overcome the problem of decoherence of quantum states.

3.3 Classical and quantum information in a quantum system

We consider the qubit state vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ from the following standpoint: How much and what (classical? quantum?) information is contained in a qubit in this state?

On posing these questions, we encounter the basic definition problems of the concept of information (classical, quantum) as applied to quantum systems. Having no way of expounding these issues in detail in our review, we propose to adopt an intuitive form of the definition of classical and quantum information contained in a qubit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The part of information that we have in the classical form we ascribe to the classical part. Indeed, when measuring the qubit in the basis $|0\rangle$, $|1\rangle$, we obtain 0 or 1. Consequently, the qubit state unknown to us contains one bit of classical information at most.

The values of the components α, β of the vector $|\psi\rangle$ are characterized by three analog quantities: the moduli $|\alpha|$ and $|\beta|$ and the phase difference $\varphi = \arg(\beta/\alpha)$.

The information contained in the amplitudes α, β can be ascribed to the quantum part of the information contained in a qubit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ [18]. The quantum part of the information cannot be obtained in a single measurement of the qubit state. To determine $|\alpha|$ and $|\beta|$ requires carrying out an infinite number of measurements over the ensemble of particles in the $|\psi\rangle$ state and determining the probabilities $p(0)$ and $p(1)$ of the test results:

$$p(0) = |\alpha|^2 \,, \qquad p(1) = |\beta|^2 \,.$$

Determining the phase difference φ requires interference-type measurements. Complete determination of the state vector is conventionally referred to as tomography of the quantum state [15].

The analog character of quantum information is of fundamental significance to the quantum theory. This is a manifestation of the fact that the manifold of quantum states forms a continuum: any two states of this continuum can be transformed to one another in a continuous manner by a unitary transformation. Hardy showed that when the system of axioms of the probability theory is complemented with the possibility of a continuous transformation of states to one another (in lieu of a jumpwise transition in the classical probability theory), quantum mechanics is interpretable as a quantum probability theory [16].

From what was stated in the preceding sections, it follows that the processes of quantum computation proceed in the space of analog variables, i.e., the amplitudes a_x at the basis states $|x\rangle$ of the system.

The quantum information theory is constructed largely by analogy with Shannon's classical information theory [15]: von Neumann's quantum entropy is constructed similarly to Shannon's informational entropy. Just as Shannon's entropy characterizes the amount of information contained (on the average) in a single signal symbol x appearing with a probability $p(x)$, so von Neumann's entropy characterizes the information in quantum states ρ_x, which stand for signal symbols and emerge with a probability $p(\rho_x)$ [15].

The properties of von Neumann's entropy are different from the properties of Shannon's entropy when we consider quantum states ρ_x with properties that are different from those of classical systems, such as incomplete distinguishability of nonorthogonal systems, entangled states of composite systems, etc. [15].

3.4 How can a quantum algorithm be realized?

The operational control of a quantum computer with n qubits is described by the transformation $|\psi_{\rm f}\rangle = {\rm U}(2^n \times 2^n)|\psi_{\rm in}\rangle$, where $|\psi_{\rm in}\rangle$ and $|\psi_{\rm f}\rangle$ are 2^n-component vectors. For $n = 10^3$, the multiplication ${\rm U}|\psi_{\rm in}\rangle$ is beyond the reach of the fastest computers (of the order of 10^{12} operations per second). The physical realization of the transformation $|\psi_{\rm in}\rangle \to |\psi_{\rm f}\rangle$ seems to be even more difficult.

The means to the realization of quantum algorithms comes to light when we consider the possibility of decomposing the matrix ${\rm U}(2^n \times 2^n)$ into an ordered product of second- and fourth-order matrices:

$$ {\rm U}(2^n \times 2^n) = \prod_{i,j} {\rm U}_i(2 \times 2) \otimes {\rm U}_j(2^2 \times 2^2)\,. \qquad (22) $$

The possibility of such a decomposition (with an accuracy sufficient for computations) is discussed at length in Ref. [15].

The second-order matrix

$$ {\rm U} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} $$

transforms the state vector

$$ \begin{vmatrix} a \\ b \end{vmatrix} $$

of one qubit:

$$ \begin{vmatrix} a' \\ b' \end{vmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{vmatrix} a \\ b \end{vmatrix}, $$

i.e., every matrix ${\rm U}_i(2 \times 2)$ in decomposition (22) describes the operation on one individual computer qubit or another. The matrices ${\rm U}(2^2 \times 2^2)$ describe the state vectors of qubit pairs:

$$ |\psi_{\rm in}\rangle = a_{00}|00\rangle + a_{10}|10\rangle + a_{01}|01\rangle + a_{11}|11\rangle \\ \to |\psi_{\rm f}\rangle = a'_{00}|00\rangle + a'_{10}|10\rangle + a'_{01}|01\rangle + a'_{11}|11\rangle\,. \qquad (23) $$

Consequently, the numbers of second- and fourth-order factors in decomposition (22) define the number of single-qubit and two-qubit operations required to realize the algorithm. For an algorithm to be efficient, the total number of operations should be a polynomial in the number of qubits 'enabled' in the computer: $N = P(n)$. When the number of operations rises exponentially with the dimension of the problem (the number of computer qubits enabled in solving a problem), the algorithm is ascribed to the class of inefficient algorithms.

3.5 Universal sets of elementary operations

Single-qubit operations describe the rotation of a single qubit:

$$ \alpha|0\rangle + \beta|1\rangle \to \alpha'|0\rangle + \beta'|1\rangle\,. $$

The character of two-qubit operations calls for additional explanation. A two-qubit operation implies an interrelation of the states of two qubits, a control, in a sense, of one (controlling) qubit over the other (controlled) qubit. Suchlike interrelation necessitates the existence of a physical interaction between the qubits, which either is engaged temporarily to execute the operation or exists permanently.

Set off from two-qubit operations is the 'Controlled NOT' — CNOT. Let the controlling qubit be the first and the controlled qubit be the second. Then, the CNOT operation is characterized by the table of input and output qubit states:

Input state	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Output state	$\|00\rangle$	$\|01\rangle$	$\|11\rangle$	$\|10\rangle$

whence it follows that the second qubit is inverted in the CNOT operation:

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

if the first is in the state $|1\rangle$. The diagrammatic symbol of the operation is presented in Fig. 6 (the time axes are shown with horizontal lines, the vertical line stands for the qubit interaction).

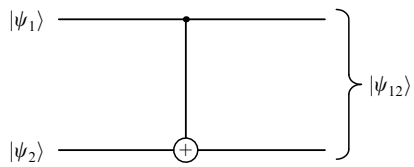

Figure 6. Schematic of the two-qubit CNOT operation. As a result of this operation, the state $|\psi_{12}\rangle$ may turn out to be entangled.

If

$$ |\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle\,, \qquad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle\,, $$

it is easy to calculate $|\psi_{12}\rangle$ with the aid of the operation table:

$$ |\psi_{12}\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|11\rangle + \beta_1\beta_2|10\rangle\,. $$

A generalization of controlled operation is the operation C-U, where U is any single-qubit operation. It is performed on the second qubit when the controlling qubit is in the state $|1\rangle$. In particular, the U operation can be a phase-change operation:

$$ {\rm U} = \begin{pmatrix} 1 & 0 \\ 0 & \exp({\rm i}\varphi) \end{pmatrix}. $$

Then,

$$ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{{\rm U}(\varphi)} \alpha|0\rangle + \exp({\rm i}\varphi)\,\beta|1\rangle\,. $$

Single-qubit operations (the continuum of state vector rotations) plus the two-qubit CNOT operation constitute the universal set of operations that make it possible to effect any transformation of a computer state vector. From the practical standpoint, the presence of the continuum operations in the set is inconvenient.

The maximum simplicity of execution is inherent in some discrete set of operations. Proposed for such a set is, for instance, the set comprising single-qubit operations: the Hadamard transformation H, the phase gate

$$ {\rm U}(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \equiv {\rm Z}\,, $$

the phase gate ${\rm U}(\pi/4)$, and the two-qubit gate CNOT [15].

The physical realization of a quantum operation is always attended with some performance inaccuracy ε. In view of this circumstance, the theory of quantum operations should be constructed as the theory of approximations.

We define the error E in the execution of the operation U as [15]

$$E(\mathrm{U},\mathrm{V}) \equiv \max_{|\psi\rangle} \left\| (\mathrm{U}-\mathrm{V})|\psi\rangle \right\| , \tag{24}$$

where U is the matrix of the ideal transformation, V is the matrix of the real (inaccurate) transformation, and $|\psi\rangle$ is the space of system space vectors. The inaccuracies of the operation sequence $\mathrm{U}_m \ldots \mathrm{U}_1$ add together in the sense of the inequality

$$E(\mathrm{U}_m \ldots \mathrm{U}_1, \mathrm{V}_m \ldots \mathrm{V}_1) \leqslant \sum_{j=1}^{m} E(\mathrm{U}_j, \mathrm{V}_j) . \tag{25}$$

We ensure the universality of the discrete set of operations $\mathrm{H}, \mathrm{T} \equiv \mathrm{U}(\pi/4), \mathrm{U}(\pi)$, and CNOT by demonstrating the possibility of effecting any single-qubit rotation U with a predetermined inaccuracy ε using these operations. We sequentially execute the operations HTH and T, which are rotations of the Bloch sphere by the angle $\pi/4$ about the Ox axis and by the angle $\pi/4$ about the Oz axis [15]:

$$\mathrm{THTH} = \exp\left(-\mathrm{i}\,\frac{\pi}{8}\,\mathrm{Z}\right) \exp\left(-\mathrm{i}\,\frac{\pi}{8}\,\mathrm{X}\right) . \tag{26}$$

A simple calculation shows that two such rotations are equivalent to one rotation $\mathrm{R}_{\mathbf{n}}(\theta)$ by the angle θ defined by

$$\cos\frac{\theta}{2} \equiv \cos^2\frac{\pi}{8} ,$$

executed about the unit vector

$$\mathbf{n}\left(\cos\frac{\pi}{8}\,,\ \sin\frac{\pi}{8}\,,\ \cos\frac{\pi}{8}\right)\left(1+\cos^2\frac{\pi}{8}\right)^{-1/2} .$$

In the second part of the demonstration, we ascertain that any angle of rotation α about the axis $\mathbf{n}$ is obtained with an error no greater than $\varepsilon/3$ by way of n rotations by the angle θ:

$$E\big(\mathrm{R}_{\mathbf{n}}(\alpha), \mathrm{R}^n_{\mathbf{n}}(\theta)\big) < \frac{\varepsilon}{3} . \tag{27}$$

The demonstration is based on the fact that the resultant angles of k rotations $\theta_k = k\theta \bmod 2\pi$ uniformly fill the space of rotation angles $(0, 2\pi)$.

Lastly, an arbitrary unitary state transformation U can be represented by three rotations about the axes $\mathbf{n}$, $\mathbf{m}$, and $\mathbf{n}$, each of which can be approximated by n_1, n_2, and n_3 rotations by a discrete angle θ:

$$E\big(\mathrm{U}, \mathbf{R}^{n_1}_{\mathbf{n}}(\theta)\mathrm{H}\mathrm{R}^{n_2}_{\mathbf{m}}(\theta)\mathrm{H}\mathrm{R}^{n_3}_{\mathbf{n}}(\theta)\big) < \varepsilon . \tag{28}$$

To attain the inaccuracy ε in the execution of a single-qubit operation, it is necessary to expend $O(\log_2^c \varepsilon^{-1})$ operations of the discrete set (the Solovei – Kitaev theorem). For the details of the calculations, the reader is referred to the encyclopedic monograph Ref. [15].

Apart from single-qubit operations, the two-qubit CNOT operation in its physical execution comprises the process of a free evolution of two qubits under the action of their interaction Hamiltonian. One qubit controls the other in the course of free evolution, the interaction energy being used in this case.

In summary, we note that an arbitrary unitary state transformation requires $O(n^2 4^n)$ operations of the universal set, i.e., the number of operations is exponentially large [15]. To be considered efficient, quantum algorithms should be executed by a polynomial number of operations.

3.6 Rabi oscillations between qubit states and single-qubit operations

For a qubit, we select a particle with the spin $I = 1/2$. The discrete spin states in a constant magnetic field $\mathbf{B} \parallel Oz$ with the energies $\hbar\omega_0 = -\mu B/2$ and $\hbar\omega_1 = +\mu B/2$ are taken as the basis qubit states:

$$|0\rangle = |\psi_{1/2}\rangle , \qquad |1\rangle = |\psi_{-1/2}\rangle .$$

The qubit is controlled by the linearly polarized variable magnetic field with the Hamiltonian

$$H_{\mathrm{int}} = -\mu I_x\, h_x(t) = -\mu I_x\, h_0 \cos(\omega t + \varphi) .$$

The field $h_x(t)$ is treated as a classical variable.

The solution of the Schrödinger equation

$$\mathrm{i}\hbar\,\frac{\mathrm{d}}{\mathrm{d}t}\,\big|\psi(t)\big\rangle = \big(-\mu I_z B - \mu I_x h_0 \cos(\omega t + \varphi)\big)\,\big|\psi(t)\big\rangle \tag{29}$$

is sought in the form of a superposition of the states $|0\rangle$ and $|1\rangle$ with variable amplitudes $C_0(t)$ and $C_1(t)$:

$$\big|\psi(t)\big\rangle = C_0(t)\,|0\rangle \exp(-\mathrm{i}\omega_0 t) + C_1(t)\,|1\rangle \exp(-\mathrm{i}\omega_1 t) . \tag{30}$$

We perform conventional calculations to arrive at the following equations for the amplitudes C_0 and C_1:

$$\begin{aligned} \dot{C}_0 &= \mathrm{i}\Omega C_1 \big[\exp(-\mathrm{i}\delta t + \mathrm{i}\varphi) + \exp\big(-\mathrm{i}(\omega + \omega_1 - \omega_0)t - \mathrm{i}\varphi\big)\big] , \\ \dot{C}_1 &= \mathrm{i}\Omega C_0 \big[\exp(-\mathrm{i}\delta t - \mathrm{i}\varphi) + \exp\big(\mathrm{i}(\omega + \omega_1 - \omega_0)t + \mathrm{i}\varphi\big)\big] . \end{aligned} \tag{31}$$

Here, $\Omega = \mu_{01} h_0/\hbar$ is the Rabi frequency ($\mu_{01} = \mu\langle 0|I_x|1\rangle = \mu/2$ is the transition matrix element) and $\delta = \omega - (\omega_1 - \omega_0)$ is the detuning of the external field frequency from resonance. The terms on the right-hand sides that oscillate at a high frequency $\omega + \omega_1 - \omega_0 \simeq 2\omega$ are commonly discarded as insignificant.

For exact resonance ($\delta = 0$) and the initial conditions $C_0(0) = 1$, $C_1(0) = 0$, the solution of the system of equations (31) is given by

$$C_0 = \cos(\Omega t) , \qquad C_1 = -\mathrm{i}\sin(\Omega t)\exp(-\mathrm{i}\varphi) . \tag{32}$$

This solution describes the stationary Rabi oscillations for the populations of the qubit states $|0\rangle$ and $|1\rangle$:

$$\big|C_0(t)\big|^2 = \frac{1}{2}\big(1 + \cos(2\Omega t)\big) , \qquad \big|C_1(t)\big|^2 = \frac{1}{2}\big(1 - \cos(2\Omega t)\big) . \tag{33}$$

By turning on the control field at a prescribed time instant, we obtain the desired magnitudes of the amplitudes C_0 and C_1; the value of the phase difference of the amplitudes

$$\arg\frac{C_1}{C_0} = \frac{\pi}{2} + \varphi$$

is then determined by the initial phase of the control field. Complete population transfer from one level to the other is effected in a time $\tau = \pi/2\Omega$:

$$\left|C_0(\tau)\right| = 0\,, \qquad \left|C_1(\tau)\right| = 1\,.$$

This operation corresponds to the execution of the NOT operator:

$$\mathrm{NOT}|0\rangle = |1\rangle\,.$$

When executing operations in a quantum computer, it is worth striving to shorten their duration. The simplest way to achieve this is to strengthen the controlling field intensity h_0 (to raise the Rabi frequency $\Omega = \mu h_0/2\hbar$). In the strong control mode ($\Omega/\omega \leqslant 1$), the rapidly oscillating terms on the right-hand side of Eqns (31) for the amplitudes C_0 and C_1 cannot be discarded. In the system of coordinates rotating with a frequency ω, the amplitudes of the qubit state vector are of the form [17]

$$\begin{vmatrix} \tilde{C}_0 \\ \tilde{C}_1 \end{vmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\mathrm{i}(\omega t + \varphi)\right) \end{pmatrix} \begin{vmatrix} C_0 \\ C_1 \end{vmatrix} = \begin{vmatrix} C_0 \\ C_1 \exp\left(\mathrm{i}(\omega t + \varphi)\right) \end{vmatrix}. \tag{34}$$

From Eqns (31), we write the equations for the amplitudes $\tilde{C}_0$ and $\tilde{C}_1$ under the condition of exact resonance ($\delta = 0$):

$$\tilde{C}_0 = \left(1 + \beta(t)\right) C_1\,, \qquad \tilde{C}_1 = \mathrm{i}\Omega\left(1 + \beta^{-1}(t)\right) C_0\,, \tag{35}$$

$$\beta(t) = \exp\left(-2\mathrm{i}\omega t - 2\mathrm{i}\varphi\right).$$

The general solution of the system is sought in the form of a power series in $\beta(t)$:

$$\tilde{C}_0 = \sum_{n=-\infty}^{+\infty} a_n \beta^n\,, \qquad \tilde{C}_1 = \sum_{n=-\infty}^{+\infty} b_n \beta^n\,. \tag{36}$$

Substituting expressions (36) in Eqns (35), we obtain the system of equations

$$\begin{aligned} a_n &= 2\mathrm{i}n\omega a_n + \mathrm{i}\Omega(b_n + b_{n-1})\,, \\ b_n &= 2\mathrm{i}n\omega b_n + \mathrm{i}\Omega(a_n + a_{n-1})\,. \end{aligned} \tag{37}$$

The small parameter of the system is the ratio $\sigma = \Omega/2\omega$.

We restrict ourselves to the part of the system $|n| \leqslant 1$, i.e., to the solution of the system with retention of the terms of the order of σ. For the initial conditions $a_0(0) = 1$, $b_0(0) = 0$, we have [17]

$$\begin{aligned} C_0(t) &= \cos(\Omega t) - \mathrm{i}\sigma \sin(\Omega t)\,\beta(t)\,, \\ C_1(t) &= \mathrm{i}\exp\left(-\mathrm{i}(\omega t + \varphi)\right)\left[\sin(\Omega t) + \sigma\cos(\Omega t)\,\beta^{-1}(t)\right]. \end{aligned} \tag{38}$$

More accurate solutions of the equations for the Rabi oscillations exhibit a high-frequency (2ω) modulation of qubit state populations (the modulation depth is $\sigma = \Omega/2\omega$). When $\sigma = \Omega/2\omega \simeq 0.1$, attaining a single-qubit operation inaccuracy of the order 10^{-4} necessitates the pulse duration to be controlled to $\Delta\tau = 1/2\omega$, which is physically hard to realize. That is why it is believed that the intensities of controlling fields should be limited by the condition $\Omega/2\omega \ll 1$.

3.7 A qubit controlled by Raman Λ-type transitions

A qubit controlled by Raman transitions of the Λ type offers several advantages, which make it popular among experimenters. The qubit energy levels are diagrammed in Fig. 7. The qubit states $|0\rangle$ and $|1\rangle$ are due to the magnetic (spin) sublevels of the ground optical state of an atom (ion) separated by intervals $E_1 - E_0$ of the order of several gigahertz. By contrast, the $|0\rangle \to |2\rangle$ and $|1\rangle \to |2\rangle$ transitions are optical transitions excited by laser pulses with the requisite polarizations and detuning δ. For the Rabi frequencies $\Omega_{02} = \Omega_{12} = \Omega \ll \delta$, the effective Rabi frequency for the $|0\rangle \to |1\rangle$ transition is $\Omega_{\mathrm{eff}} = \Omega^2/\delta$. Under these conditions, the high-frequency modulation depth of the state population is small: $\sigma = \Omega_{\mathrm{eff}}/2\omega_{02} \ll 1$. The attainment of high-accuracy control of a Λ-type qubit may prove to be its important advantage in experiments [17].

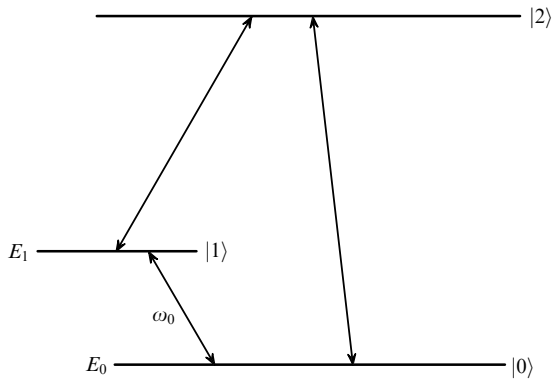

Figure 7. Qubit control with the aid of optical transitions by the Raman scheme.

4. Mixed and entangled states of quantum systems

4.1 Mixed states of quantum systems

Ensembles of quantum systems prepared in a specific way are quite often handled in experiments. From the standpoint of description of the particle states in an ensemble, a system can be prepared in two ways: (i) with acquisition of complete information on the state of the quantum system; (ii) with acquisition of only probabilistic information on the state of the quantum system. These ways of preparation are exemplified in Fig. 8. A furnace produces a stream of atoms (qubits) with the spin $I = 1/2$; the states $|0\rangle$ (spin up) and $|1\rangle$ (spin down) are encountered in the atomic ensemble with the Boltzmann probability distributions.

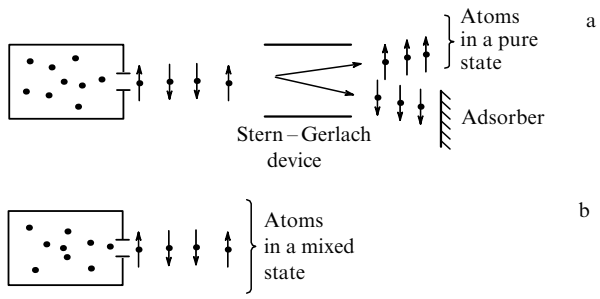

Figure 8. Scheme for preparing atoms in pure (a) and mixed (b) states.

In the first method of preparation, an ensemble of atoms passes through a separator (a Stern–Gerlach device), which spatially divides it into two streams corresponding to the states $|0\rangle$ and $|1\rangle$. The ensemble of atoms in the state $|1\rangle$ is absorbed by an adsorber; the remaining ensemble of atoms is in the pure state $|0\rangle$. Therefore, we have complete information on the state of atoms in the ensemble. In the second method, the separator is absent; the ensemble of atoms consists of atoms in the states $|0\rangle$ or $|1\rangle$ with the probabilities $p_{|0\rangle}$ or $p_{|1\rangle}$. Such a state is a mixture of the pure states $|0\rangle$ and $|1\rangle$.

Mathematically, a mixed state of a quantum system can be described only by the density matrix

$$\rho = p_{|0\rangle}|0\rangle\langle 0| + p_{|1\rangle}|1\rangle\langle 1|\,, \tag{39}$$

where

$$|0\rangle\langle 0| = \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}, \qquad |1\rangle\langle 1| = \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix}$$

are the operators of projection on the states $|0\rangle$ and $|1\rangle$. It is valid to say that the quantum system in a mixed state does not have a wave function [19]. The density matrix does not contain information about the phases of the states that make up the mixture. This implies that mixed states are not quantum-coherent; they do not exhibit quantum interference effects. Mixed states may be classified as close-to-classical states, because their description by the density matrix is close to the statistical description of classical systems.

Many authors consider the passage from pure states to mixed states as the classicization process of quantum-coherent systems. However, the states that make up the mixture are quantum-coherent; in particular, they may be entangled, and this entanglement can be extracted from the mixed state (entanglement purification) and transmitted to another quantum system in a pure state [14].

The transition of a system from a quantum-coherent pure state, which is described by its wave function, to an incoherent state, described by a density matrix, is also referred to as the process of decoherence of the system.

4.2 Mixed states of quantum subsystems

Quantum systems are often composite systems: they consist of two or more subsystems. Even when the system as a whole is in a pure state (described by a wave function), its constituent subsystems may be in a mixed state and be described by a density matrix. This is the case if the pure state of a system is the so-called entangled state of the subsystems that constitute the system.

We exemplify this by a composite system containing qubits A and B. We execute two successive unitary transformations of this system, with the effect that the two qubits find themselves in an entangled state:

$$\left|\psi_{AB}^{(\mathrm{in})}\right\rangle = |0_A\rangle|0_B\rangle \xrightarrow{\mathrm{H}_1} \frac{1}{\sqrt{2}}\left(|0_A\rangle + |1_A\rangle\right)|0_B\rangle$$

$$\xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{2}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle\right) \equiv \left|\psi_{AB}^{(\mathrm{f})}\right\rangle. \tag{40}$$

The final state

$$\left|\psi_{AB}^{(\mathrm{f})}\right\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle\right)$$

is entangled because it cannot be represented as the product of the wave functions of qubits A and B:

$$\left|\psi_{AB}^{(\mathrm{f})}\right\rangle \neq |\psi_A\rangle|\psi_B\rangle\,.$$

It is impossible to choose

$$|\psi_A\rangle = \alpha_A|0\rangle + \beta_A|1\rangle\,, \qquad |\psi_B\rangle = \alpha_B|0\rangle + \beta_B|1\rangle\,,$$

such that the equality

$$\left|\psi_{AB}^{(\mathrm{f})}\right\rangle = |\psi_A\rangle|\psi_B\rangle$$

holds. But it is possible to find density matrices that describe qubits A and B separately. The density matrix of the composite system AB is

$$\rho_{AB} = \left|\psi_{AB}^{(\mathrm{f})}\right\rangle\left\langle\psi_{AB}^{(\mathrm{f})}\right| = \frac{1}{2}\left[|0_A\rangle\langle 0_A||0_B\rangle\langle 0_B| + |0_A\rangle|0_B\rangle\langle 1_A|\langle 1_B| + |1_A\rangle|1_B\rangle\langle 0_A|\langle 0_B| + |1_A\rangle|1_B\rangle\langle 1_A|\langle 1_B|\right]. \tag{41}$$

We find the reduced density matrix for qubit A:

$$\rho_A = \mathrm{Tr}_B\,\rho_{AB} \equiv \langle 0_B|\rho_{AB}|0_B\rangle + \langle 1_B|\rho_{AB}|1_B\rangle = \frac{1}{2}\left(|0_A\rangle\langle 0_A| + |1_A\rangle\langle 1_A|\right) = \frac{1}{2}\,\mathrm{I}\,, \tag{42}$$

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

A similar result is obtained for qubit B:

$$\rho_B = \frac{1}{2}\,I\,.$$

The states of qubits A and B turn out to be mixed; the mixture is made up of the pure states $|0\rangle$ and $|1\rangle$ with the probabilities $p_{|0\rangle} = p_{|1\rangle} = 1/2$.

In classical physics, the information that provides a complete description of the system as a whole is also sufficient for the complete description of its parts. In quantum mechanics, this rule breaks down when the whole is in the so-called entangled state: the information that gives a complete description of the whole is insufficient for the complete description of the parts making up the whole.

4.3 Entangled states of quantum systems

The theory of entangled states of composite quantum systems is in the development stage. As regards systems comprising two parts (A and B), a more or less complete understanding and description of entanglement has been obtained. The propositions of the theory of two-particle systems defy attempts at direct extension to systems made up of more than two parts. Several particular results have been obtained for such systems. Some of them are considered below.

Entanglement is the crucial property of quantum systems. The existence of entangled systems implies the nonlocality of the quantum description of nature [15]. Entanglement is the most important resource in quantum informatics: employing entangled states underlies the execution of the protocols of quantum teleportation, cryptography, and computation. The phenomenon of entanglement therefore attracts considerable interest from researchers. It is surprising that no mention is made of entanglement in quantum systems in conventional textbooks on quantum mechanics [19], although entangled

states were discovered in 1935 in the famous works of Schrödinger [20], Einstein et al. [21].

We consider a two-component quantum system A and B in a pure state $|\psi_{AB}\rangle$. Let A and B be distinguishable (nonidentical particles[3]) and let the dimensions of subsystems A and B be M and N ($M \leqslant N$).

The $|\psi_{AB}\rangle$ state vector can be decomposed in terms of the basis functions u_i and v_i of subsystems A and B (the Schmidt decomposition):

$$|\psi_{AB}\rangle = \sum_{i=1}^{M} c_i |u_i\rangle |v_i\rangle \,. \tag{43}$$

The number of nonzero coefficients c_i in the decomposition is the Schmidt number Sch. If Sch $= 1$, the state $|\psi_{AB}\rangle = |u\rangle|v\rangle$ is not entangled, because it is the product of states u and v of the subsystems. If Sch $\geqslant 2$, the $|\psi_{AB}\rangle$ state is entangled.

For a system described by a density matrix ρ, von Neumann's entropy

$$S(\rho) = -\mathrm{Tr}\,(\rho \log_2 \rho) \tag{44}$$

can measure the entanglement in a two-component system [22]. A pure state $|\psi_{AB}\rangle$ is completely defined, and hence $S(\rho_{AB}) = 0$. However, the states of subsystems A and B taken separately are characterized by the uncertainty being expressed in terms of the probabilities $|c_i|^2$ in the density matrices:

$$\begin{aligned} \rho_A &= \mathrm{Tr}_B\, \rho_{AB} = \sum_i \langle v_i|\rho_{AB}|v_i\rangle = \sum_i |c_i|^2 |u_i\rangle\langle u_i| \,, \\ \rho_B &= \sum_i |c_i|^2 |v_i\rangle\langle v_i| \,. \end{aligned} \tag{45}$$

The values of von Neumann's entropy for subsystems A and B are positive:

$$S(\rho_A) = S(\rho_B) = -\sum_i |c_i|^2 \log_2 |c_i|^2 > 0 \,. \tag{46}$$

The uncertainty in the states described by the density matrices ρ_A and ρ_B exists prior to the measurement of the states of subsystems A and B. The greater this uncertainty, the greater the entanglement in the state $|\psi_{AB}\rangle$ of the composite system AB. For a qubit described by the density matrix

$$\rho_A = |c_0|^2 |0\rangle\langle 0| + |c_1|^2 |1\rangle\langle 1| \,,$$

the maximum $S(\rho_A) = 1$ is attained for $|c_0|^2 = |c_1|^2 = 1/2$. This corresponds to the pure state

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

of a two-qubit composite system, which has the greatest entanglement in the system of qubits A and B.

Therefore, the measure of entanglement in the pure state $|\psi_{AB}\rangle$ of the composite system AB is the measure of uncertainty of the states of subsystems A and B — von Neumann's entropy. For different subsystems, all the uncertainty in ρ_A and ρ_B is due to the entanglement in the state $|\psi_{AB}\rangle$.

[3] The identity of particles introduces new elements in the entanglement theory for fermions and bosons (see below).

For identical particles A and B in the states ρ_A and ρ_B, there arise additional uncertainties caused by their identity. For fermions with a spin I, the Schmidt decomposition is performed in terms of antisymmetrized combinations of the basis functions $|2i-1\rangle$ and $|2i\rangle$ [22]:

$$|\psi_{AB}\rangle = \sum_{i=1}^{(2I+1)/2} a_i \frac{1}{\sqrt{2}}\big(|2i-1\rangle_A |2i\rangle_B - |2i\rangle_A |2i-1\rangle_B\big) \,. \tag{47}$$

It is easy to find the reduced density matrix ρ_A (or ρ_B) and von Neumann's entropy $S(\rho_A) = S(\rho_B)$ in this case:

$$\begin{aligned} \rho_A &= \mathrm{Tr}_B\,\big(|\psi_{AB}\rangle\langle\psi_{AB}|\big) \\ &= \sum_{i=1}^{(2I+1)/2} \frac{1}{2}\,|a_i|^2 \big(|2i-1\rangle_A\langle 2i-1|_A + |2i\rangle_A\langle 2i|_A\big) \,, \\ S(\rho_A) &= -\mathrm{Tr}\,(\rho_A \log_2 \rho_A) = -\sum_i |a_i|^2 \log_2 \frac{|a_i|^2}{2} \\ &= 1 - \sum_i |a_i|^2 \log_2 |a_i|^2 \,. \end{aligned} \tag{48}$$

Expression (48) implies that von Neumann's entropy $S(\rho_A) \geqslant 1$ for all $|a_i|^2 \in [0,1]$, $\sum_i |a_i|^2 = 1$. The minimal value $S(\rho_A) = 1$ is due to the uncertainty in the state ρ_A arising from the particle identity. In this case, the Schmidt number Sch $= 1$ and the state

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\big(|1_A\rangle|2_B\rangle - |2_A\rangle|1_B\rangle\big)$$

is not entangled:

$$\rho_A = \frac{1}{2}\big(|1_A\rangle\langle 1_A| + |2_A\rangle\langle 2_A|\big) \,, \qquad S(\rho_A) = 1 \,.$$

The final result for fermions is that if the Schmidt number for the state $|\psi_{AB}\rangle$ is Sch $= 1$ or $S(\rho_A) = 1$, which is equivalent, the $|\psi_{AB}\rangle$ state is not entangled; if Sch > 1 or $S(\rho_A) > 1$, then $|\psi_{AB}\rangle$ describes an entangled state of the fermions.

The following results were obtained for bosons [22]: the state $|\psi_{AB}\rangle$ is not entangled if

(1) Sch $= 1$, $S(\rho_A) = S(\rho_B) = 0$,

(2) Sch $= 2$, $S(\rho_A) = S(\rho_B) = 1$;

the $|\psi_{AB}\rangle$ state is entangled if

(1) Sch $= 2$, $S(\rho_A) = S(\rho_B) \in (0,1)$,

(2) Sch > 2, $S(\rho_A) = S(\rho_B) \in \big(0, \ln(2S+1)\big)$.

Hence, it is clear that the entanglement criteria of the state $|\psi_{AB}\rangle$ of identical particles include both the values of the Schmidt number for $|\psi_{AB}\rangle$ and the values of von Neumann's entropy for subsystems $S(\rho_A) = S(\rho_B)$.

4.4 Transformations of entangled states

Considering entanglement as a resource, we should be able to produce (generate), store, transform, and employ it. We now direct our attention to the issue of entangled-state transformations. Let the parts $A, B, C, \ldots$ of an entangled system be located at different points in space at the disposal of subjects S_A, S_B, $S_C, \ldots$ Each of the subjects can perform local operations on their own part of the system and report it to other subjects using a classical communication channel

LOCC (Local Operations — Classic Communications). A development of the idea of LOCC is a stochastic LOCC (SLOCC), when the transformation $|\psi\rangle \to |\varphi\rangle$ is possible with a finite probability. Borne in mind in this case are operations involving a single system rather than an ensemble of systems.

By way of LOCC (SLOCC) type operations, it is possible to transform the initial entangled system state $|\psi\rangle$ to another entangled state $|\varphi\rangle$. An important example of such transformations is entanglement distillation, i.e., preparation of extremely entangled systems from partially entangled (not as much as possible) systems. Performed by LOCC-type operations is the protocol of quantum state teleportation, when subjects S_A and S_B, who perform the protocol, have a pair of extremely entangled qubits at their disposal. The two states $|\psi\rangle$ and $|\varphi\rangle$ of the composite system are transformed into each other by LOCC if they are related to each other by a local unitary matrix: $|\varphi\rangle = \mathrm{U}_{\mathrm{loc}}|\psi\rangle$.

For a two-particle system AB, we write

$$|\varphi_{AB}\rangle = \mathrm{U}_A \otimes \mathrm{U}_B|\psi_{AB}\rangle = \sum_{i=1}^{n_\psi} \sqrt{\lambda_i}\,|i_A\rangle|i_B\rangle\,, \tag{49}$$

where U_A and U_B are the local transformation matrices, the right-hand side of (49) is represented in the form of the Schmidt decomposition, and n_ψ is the Schmidt number for the vector $|\psi_{AB}\rangle$ invariant under LOCC.

For a two-particle system $\mathrm{H}_A^{(n)} \otimes \mathrm{H}_B^{(m)}$ ($n \leqslant m$ are the dimensions of subsystems A and B), the values $n_\psi = 1, \ldots, n$. This implies that there exist n classes of nonequivalent (not transformable into each other by LOCC) states $|\psi_{AB}\rangle$.

A system of two qubits ($n = m = 2$, $n_\psi = 1, 2$) has two nonequivalent classes of states:

$$n_\psi = 1\,, \quad |\psi_{AB}\rangle = |1_A\rangle|1_B\rangle \quad \text{(nonentangled)},$$
$$n_\psi = 2\,, \quad |\varphi_{AB}\rangle = \lambda_1^{1/2}|1_A\rangle|1_B\rangle + \lambda_2^{1/2}|2_A\rangle|2_B\rangle \quad \text{(entangled)}.$$

It is clear that a nonentangled state cannot be transformed into an entangled one by LOCC-type operations. The states belonging to nonequivalent classes may be related by nonlocal operations (of the CNOT type) or by irreversible local operations including, for instance, measurements.

The systems consisting of three particles A, B, C have six classes of nonequivalent states [23]: the nonentangled state $|\psi_A\rangle|\psi_B\rangle|\psi_C\rangle$; classes $A - BC$, $AB - C$, $CA - B$, in which two particles out of three are entangled; and two nonequivalent classes of states wherein all three particles are entangled. For three qubits, the states can be written as

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big)\,,$$
$$|W\rangle = \frac{1}{\sqrt{3}}\big(|100\rangle + |010\rangle + |001\rangle\big)\,.$$

The consideration of the entangled states of three or more particles brings up the question: to what extent can an object (a qubit) be entangled simultaneously with two (or more) objects? It turns out that quantum entanglement (quantum correlations) cannot freely emerge (be produced) between one object and many others (unlike classical correlations). For instance, in the system of three particles A, B, and C, the existence of entanglement of A with B implies that the entanglement of A with C is bounded from above [24].

Generalizing the state $|\mathrm{GHZ}\rangle$ to the case of $n \gg 1$ qubits, we obtain a state like 'Schrödinger's cat':

$$|\psi_n\rangle = \frac{1}{\sqrt{2}}\big(|0_1 \ldots 0_n\rangle + |1_1 \ldots 1_n\rangle\big)\,,$$

which is the model of the state of a macroscopic body in a superposed quantum state. By investigating the processes of decoherence of a state $|\psi_n\rangle$, it is possible to answer the fundamental question: why do macroscopic bodies behave as classical bodies, while they are actually quantum (in the sense that the quantum description of large-dimension bodies is not prohibited). Section 7, which is concerned with decohering processes, provides the answer to this question.

4.5 Entanglement in the mixed states of composite systems

Mixed states of a two-particle system are described by a density matrix of the form

$$\rho^{AB} = \sum_i p_i\,\rho_i^{AB} = \sum_i p_i\,\big|\psi_i^{AB}\big\rangle\big\langle\psi_i^{AB}\big|\,, \tag{50}$$

where p_i is the probability that the system in the state $\rho_i^{AB} = \big|\psi_i^{AB}\big\rangle\big\langle\psi_i^{AB}\big|$ is found in the ensemble. When all ρ_i^{AB} are factorable ($\rho_i^{AB} = \rho_i^A \otimes \rho_i^B$), the mixed state contains no entanglement. When some of the states ρ_i^{AB} are not factorable (are entangled), the mixed state ρ_{AB} as a whole contains entanglement, the amount of which may be defined by the formula [14]

$$E(\rho_{AB}) = \min \sum_i p_i\,S(\rho_i^A)\,, \tag{51}$$

where $S(\rho_i^A)$ is von Neumann's entropy for the subsystem A in the state $\rho_i^A = \mathrm{Tr}_B\,\rho_i^{AB}$.

The interest in entanglement in mixed states arises from the possibility of purifying this entanglement and preparing, at its expense, extremely entangled pairs in a pure state. Protocols of such purification have been proposed [14].

4.6 Experimental methods of obtaining entangled states

Entanglement as a resource is an expendable factor. Consequently, methods for 'preparing' entangled pairs are required. Using the unitary two-qubit transformation CNOT, from the initial nonentangled state of two qubits

$$\frac{1}{\sqrt{2}}\big(|0_A\rangle + |1_A\rangle\big)|0_B\rangle\,,$$

we obtain the extremely entangled pair of qubits

$$\frac{1}{\sqrt{2}}\big(|0_A\rangle|0_B\rangle + |1_A\rangle|0_B\rangle\big) \xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}\big(|0_A\rangle|0_A\rangle + |1_A\rangle|1_B\rangle\big)\,. \tag{52}$$

This method may be termed algorithmic, because the operations employed were borrowed from the universal set intended for executing quantum algorithms. Entangled qubits with ions in a trap [5] and nuclear spins in an NMR quantum computer [25] were obtained by the algorithmic method.

In the majority of experiments in entanglement, use is made of photon pairs produced due to the spontaneous decay of an ultraviolet pump photon in a nonlinear crystal — the

so-called down-conversion [26]. Produced in the down-conversion are a signal (s) photon and an idle (i) photon. From the conservation laws, it follows that $\mathbf{k}_{\rm ph} = \mathbf{k}_{\rm s} + \mathbf{k}_{\rm i}$ and $\omega_{\rm ph} = \omega_{\rm s} + \omega_{\rm i}$.

The wave function of the photons can be written as a superposition of the products of single-photon pure states $|\omega_{\rm s}\rangle_{\rm s}|\omega_{\rm ph} - \omega_{\rm s}\rangle_{\rm i}$ in the frequency representation with the amplitudes $\Phi(\omega_{\rm ph}, \omega_{\rm s}, \omega_{\rm i})$ [27]:

$$|\psi\rangle_{\rm ph} = M|{\rm vac}\rangle_{\rm s}|{\rm vac}\rangle_{\rm i} + \eta\upsilon \sum_{\omega_{\rm s}} \Phi(\omega_{\rm ph}, \omega_{\rm s}, \omega_{\rm i})|\omega_{\rm s}\rangle_{\rm s}|\omega_{\rm ph} - \omega_{\rm s}\rangle_{\rm i}\,, \qquad (53)$$

where $\eta\upsilon \ll 1$ is the conversion coefficient. In the absence of the pump, the oscillators $\omega_{\rm s}$, $\omega_{\rm i}$ are in the vacuum state $M \simeq 1$. By varying the generation conditions, it is possible to obtain photon pairs entangled in polarization, momentum, or time [27].

In a broader sense, the decay of any particle in the singlet state into two particles produces pairs of particles entangled in coordinate, momentum, or spin:

$$\begin{aligned} |\psi_{\rm in}\rangle &= \delta(\mathbf{x}) \to \frac{1}{\sqrt{2}}\left(|x_1\rangle_A|x_2\rangle_B + |x_1\rangle_B|x_2\rangle_A\right), \\ |\psi_{\rm in}\rangle &= \delta(\mathbf{p}) \to \frac{1}{\sqrt{2}}\left(|p_1\rangle_A|p_2\rangle_B + |p_1\rangle_B|p_2\rangle_A\right), \qquad (54) \\ |\psi_{\rm in}\rangle &= |S_0\rangle \to \frac{1}{\sqrt{2}}\left(|0_A\rangle|1_B\rangle + |0_B\rangle|1_A\rangle\right). \end{aligned}$$

The methods reliant on the decay of particles in the singlet state may be termed 'physical'.

5. Problems of qubit state measurements

5.1 Qubit state measurement

Measurement of the qubit states in a quantum computer is considered to be one of the routine operations. For instance, the qubits of a quantum register may be algorithmically initialized: every qubit in the unknown state of the register $|\psi\rangle = \sum_x a_x|x\rangle$ is subjected to measurement in the basis $|0\rangle$, $|1\rangle$. When $|0\rangle$ results, the qubit initialization is accomplished; when $|1\rangle$ results, the NOT$|1\rangle = |0\rangle$ operation is applied. The operation of measurement is performed in the course of error correction process (reading of error syndrome) and return of ancillary qubits to the state $|0\rangle$. Lastly, the measurement of all qubits of the quantum register in the basis $|0\rangle$, $|1\rangle$ is performed with the aim of obtaining classical information (the binary number $j_1, \ldots, j_n = \{0, 1\}$) on the solution of the problem upon completion of computations.

From the theoretical standpoint, the procedure of measuring the qubit state in the basis $|0\rangle$, $|1\rangle$ is not associated with any difficulties. However, the physical realization of qubit measurement involves the solution of extremely complex technological problems associated with overcoming the difficulties of measuring the state of an individual atomic particle: atom, ion, electron, electron or atomic nuclear spin, or photon. Actually, each qubit realization calls for the development of a specific physical method for the measurement of the qubit state. We show how this can be accomplished for the qubits on the basis of the optical levels of an ion in a trap [5].

For the $|0\rangle$ qubit state, we select the $4\,^2S_{1/2}$ sublevel of the ground state, and the $3\,^2D_{5/2}$ sublevel of an excited metastable state is adopted as the $|1\rangle$ state (see Fig. 3). The 'interrogation' of an ion may be effected by a laser with the wavelength $\lambda = 397$ nm, which excites the $4\,^2S_{1/2} \to 4\,^2P_{1/2}$ dipole transitions. When the qubit is in the $|0\rangle = |4\,^2S_{1/2}\rangle$ state, it transits to the $|2\rangle = |4\,^2P_{1/2}\rangle$ state under laser irradiation. The qubit's return to the $|0\rangle$ state (spontaneous transition) is attended with the emission of a photon, which provides the information that the qubit was in the $|0\rangle$ state at the instant of the beginning of measurement. If the ion was in the $|1\rangle = |3\,^2D_{5/2}\rangle$ state prior to the measurement, no photon emission occurs. From the $4\,^2P_{1/2}$ state, the ion may spontaneously transit to the metastable $3\,^2D_{3/2}$ level. To eliminate the ion 'trapping' in this state, one more laser at the $3\,^2D_{3/2} \to 4\,^2P_{1/2}$ transition frequency ($\lambda = 866$ nm) is engaged in the measurement, which precludes the population trapping in the $|3\,^2D_{3/2}\rangle$ level.

The detector of spontaneously emitted photons has a small angular dimension ($\Omega \ll 4\pi$), and therefore the single-photon detection efficiency is $\eta \ll 1$. If N photons are emitted as a result of the cyclic transitions $|0\rangle \to |2\rangle$ (under laser irradiation with the wavelength $\lambda = 397$ nm) and $|2\rangle \to |0\rangle$ (spontaneous transition), the detector records $n = \eta N$ photons on the average. The probability that none of the N photons is detected is $p_N(0) = (1-\eta)^N = \exp(-n)$. For $n = 10$, this probability is $p_N(0) = 4.5 \times 10^{-5}$, i.e., for $n \gg 1$, the probability of error in the measurement is low (the state $|0\rangle$ was adopted as $|1\rangle$).

If the qubit is in a superposition state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ at the instant the measurement begins, the population $|\alpha|^2$ of the state $|0\rangle$ operates in the measurement: $N \propto |\alpha|^2$. The population $|\beta|^2$ of state $|1\rangle$ is trapped in the metastable level and is 'inactive'.

We emphasize the statistical nature of the measurement and the need for lengthening the measurement time so as to make the number of photons detected $n = \eta N$ statistically large. Unfortunately, this property (the need for signal accumulation) is inherent in the majority of techniques developed for measuring the state of individual atomic particles.

In principle, it is desirable that the duration of measurement be comparable to the duration of quantum operations. In this case, the measurement could be employed as a routine computational operation. In the course of long-duration measurements (the methods involving signal accumulation), precautions must be taken to retain the quantum coherence of the state being measured.

Without going into detail, we consider a possible method for measuring the state of qubits on the basis of a single spin $I = 1/2$. The theory of a method involving a magnetic-resonance force microscope is being actively developed [28]. The magnetic dipole – dipole interaction of an individual spin with the dipole of a ferromagnetic probe at the tip of a mechanical resonator cantilever is used for the resonance excitation of cantilever vibrations. When the spin experiences a sufficiently long periodic sequence of π pulses, cantilever vibrations are excited, which are detected by optical methods.

For spins in a solid (the $I = 1/2$ nuclear spins of phosphorus ^{31}P in a spinless single crystal of silicon ^{28}Si), multistage methods were proposed for measuring the state of the nuclear spin: the information about the nuclear spin state is transmitted to the electron spin S of the ^{31}P atom; from the spin S, the information is transmitted to the electron charge e.

The presence (absence) of a single electron charge in the vicinity of a nanotransistor is detected by measuring the current through the nanotransistor [29].

Although each of the above-listed 'relay race' appears to be feasible, these stages have never been realized all together. In NMR quantum computers, which make use of the technique of pulsed magnetic resonance in molecular liquids at room temperature, the detectable signal is produced by a macroscopic ensemble (of the order of 10^{18}) molecules. Estimates show that the technique of pulsed NMR in a solid at low temperatures ($T < 0,1$ K) would enable signal detection from an ensemble of about 10^6 atoms [30].

Measurements of the state of qubits made around superconducting mesostructures (quantum dots with Cooper pairs or SQUIDs with supercurrents) reduce to electrical measurements with signal accumulation [31, 32].

It is safe to say that the problem of individual qubit state measurement is among the most difficult from the viewpoint of the physical realization of a quantum computer.

5.2 Tomography of a qubit state

The procedure for determining the density matrix ρ of the unknown state of a system is termed the tomography of a quantum state [15]. The quantum state tomography is a substantial development of the idea of measuring the quantum state of the system in some basis. The measurement of a state $|\psi\rangle = \sum_x c_x|x\rangle$ in the basis $|x\rangle$ is performed on a single specimen of the system. The measurement result is some basis state $|x\rangle$ with the probability $|c_x|^2$. In a single measurement, the probabilities $|c_x|^2$ remain unknown.

The state tomography implies that it is necessary to determine all elements of the matrix ρ or (for a system in a pure state $|\psi\rangle = \sum_x c_x|x\rangle$) all the amplitudes c_x, including their phases. The state tomography is a statistical procedure that requires the presence (preparation) of an unlimited ensemble of particles in the state ρ and the performance of measurements on the particles of this ensemble. Through the example of a qubit, we consider what measurements are required.

The density matrix ρ of a qubit can be expanded in terms of the usual set of the matrices of qubit transformation operators I, X, Y, Z:

$$\rho \equiv \mathrm{Tr}\,(\mathrm{I}\rho)\mathrm{I} + \mathrm{Tr}\,(\mathrm{X}\rho)\mathrm{X} + \mathrm{Tr}\,(\mathrm{Y}\rho)\mathrm{Y} + \mathrm{Tr}\,(\mathrm{Z}\rho)\mathrm{Z}\,. \quad (55)$$

The quantity $\mathrm{Tr}\,(\mathrm{A}\rho)$ is the mean value of the observable A.

From Eqn (55), it follows that determining the density matrix ρ of an unknown state requires statistical measurements that enable determination of the average values (first-order moments) of the observables X, Y, and Z:

$$\langle \mathrm{X}\rangle = \mathrm{Tr}\,(\mathrm{X}\rho) \equiv \lim_{m\to\infty}\left(\frac{1}{m}\sum_{i=1}^{m}\mathrm{X}_i\right), \quad \ldots \quad (56)$$

The (approximate) values of qubit ρ-matrix elements found from the measurements are given by

$$\rho_{11} = 1 + \langle \mathrm{Z}\rangle\,, \quad \rho_{12} = \rho_{21}^* = \langle \mathrm{X}\rangle - \mathrm{i}\langle \mathrm{Y}\rangle\,, \quad \rho_{22} = 1 - \langle \mathrm{Z}\rangle\,. \quad (57)$$

The distribution of $\langle \mathrm{X}\rangle$ and the value of the root-mean-square deviation of $\langle \mathrm{X}\rangle$ follow from the central limit theorem [15].

The generalization of quantum state tomographic procedure to systems containing n qubits (a quantum computer) is evident:

$$\rho = 2^{-n}\sum \mathrm{Tr}\,(O_1 \otimes \ldots \otimes O_n \otimes \rho)(O_1 \otimes \ldots \otimes O_n)\,, \quad (58)$$
$$O \in (\mathrm{I}, \mathrm{X}, \mathrm{Y}, \mathrm{Z})\,.$$

The procedure of 'tomography of a quantum process' was proposed on the basis of the quantum state tomographic procedure. For instance, in the operation of a quantum computer, its qubits are subjected to decohering effects, whose operator E is unknown. We now illustrate the idea of the method of quantum process tomography by the example of one qubit. We select $d^2 = 4$ ($d = 2$ is the dimension of the qubit state space) of the subensemble of qubits in the basis states $\rho_1, \ldots, \rho_4$:

$$\rho_1 = |\psi_1\rangle\langle\psi_1|, \quad \ldots, \quad \rho_4 = |\psi_4\rangle\langle\psi_4|\,.$$

As a result of an unknown decoherence process characterized by the operator E, the states ρ_i are transformed:

$$\rho_i \to \rho_i' = \mathrm{E} \otimes \rho_i\,.$$

The states ρ_i are known, and the states with errors ρ_i' are determined using the procedures of quantum state tomography. Then, the equalities

$$\rho_i' = \mathrm{E} \otimes \rho_i$$

are the system of equations for determining the elements of the unknown matrix E. For the mathematical details, the reader is referred to Ref. [9].

6. Quantum algorithms

6.1 Quantum algorithms of number factorization and database search

To date, three classes of quantum algorithms have been discovered and comprehensively investigated: (1) algorithms with quantum hidden subgroups of the Abelian transformation group (among them is Shor's number factorization algorithm [9]); (2) algorithms with amplitude amplification (represented by Grover's algorithm for object search in an unstructured database [33]); (3) algorithms for modeling quantum systems with a quantum computer [15, 34–36].

Class-(1) and (3) algorithms imply the application of a discrete Fourier transformation. Performing the Fourier transformation with a classical computer requires an exponentially large number of operations. With a quantum computer, the Fourier transformation is performed in a polynomial number (n^2) of operations. That is why class-(1) and (3) algorithms demonstrate an exponential acceleration of problem solving in comparison with the algorithms executed with classical computers.

The principle of Grover's algorithm is the amplitude amplification of the state corresponding to the desired object. Let an integer x_s be the index of the desired object. We associate it with the basis state $|x_s\rangle$ in the state vector $|\psi\rangle = \sum_x c_x|x\rangle$ of the quantum register. The iterative procedure in the performance of Grover's algorithm is constructed such that the interference of amplitudes increases the amplitude c_{x_s}; the remaining amplitudes $c_{x\neq x_s}$ are decreased. Upon $\sqrt{N}$ iterations (N is the number of objects in the database), the amplitude c_{x_s} reaches a value $|c_{x_s}| \leqslant 1$.

Measurement of the register state upon $\sqrt{N}$ iterations (operations) defines the index x_s of the desired object with a probability $|c_{x_s}|^2 \simeq 1$. The object search in the classical case requires N operations (exhaustive search). Quantum Grover's algorithm is therefore said to achieve a quadratic acceleration of search problem solving.

Mathematicians investigate the possibility of constructing new classes of efficient quantum algorithms, for instance, for the solution of the so-called isomorphism of graphs [37]. The greater the number of efficient quantum algorithms found, the more incentives to realize the idea of quantum computers. The possibility of efficiently solving the problems of quantum physics is a good reason to develop a quantum computer.

Below, we provide examples of quantum teleportation algorithms and outline the approaches to the algorithms for modeling quantum systems. The first example allows one to become aware of the details that make up quantum algorithms; the second example is of prime interest to the physicist-reader.

6.2 Teleportation algorithm for an unknown quantum state

An instructive example of a low-dimensional algorithm is the protocol of quantum teleportation of an unknown quantum state [38]. The teleportation protocol is diagrammed in Fig. 9. Initially, three qubits participating in the protocol are at a point A and their state is not entangled:

$$|\psi_{\text{in}}\rangle = |a_1\rangle|0_2\rangle|0_3\rangle\,.$$

Here, $|a_1\rangle = \alpha|0_1\rangle + \beta|1_1\rangle$ is the unknown state of qubit 1. It is precisely this state that should be teleported to a point in space B. The events occurring at points A and B are framed in Fig. 9.

The first operation produces entanglement of qubits 2 and 3. The operation is performed in two stages: the Hadamard transformation H and then CNOT_{23} are performed on the state of qubit 2:

$$|0_2\rangle|0_3\rangle \xrightarrow{\text{H}_2} \frac{1}{\sqrt{2}}\big(|0_2\rangle + |1_2\rangle\big)\,|0_3\rangle \xrightarrow{\text{CNOT}_{23}} \frac{1}{\sqrt{2}}\big(|0_2 0_3\rangle + |1_2 1_3\rangle\big)\,. \tag{59}$$

The entanglement of qubits 2 and 3 is shown in the diagram with a spiral connection between the lines of time evolution. Upon generation of the entanglement of qubits 2 and 3, qubit 3 is transported to point B, which is at an arbitrary distance from point A.

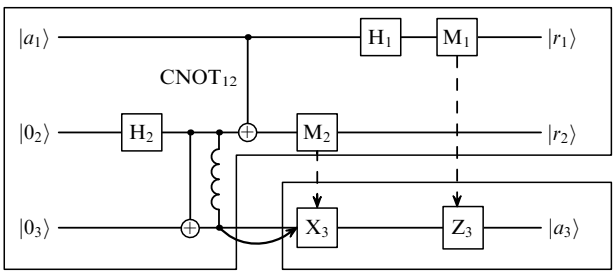

Figure 9. Schematic of the protocol of teleportation of an unknown state $|a_1\rangle$ from point A to point B. Entanglement is produced in the course of teleportation and is later destroyed during qubit state measurements. In addition, one of the qubits of the entangled pair is transported from point A to point B.

Subsequent local-type operations (LOCC) are performed on qubits 1 and 2 at point A and on qubit 3 at point B. The dashed lines show the transmission of classical information to point B on the result of measurement of the qubit state at point A. This information is used to perform operations (X_3 or Z_3) on qubit 3 at point B.

In the second operation, the entanglement of qubits 2 and 3 is transformed into the entanglement of qubits 1 and 3 with the participation of all three qubits:

$$\begin{aligned}&\frac{1}{\sqrt{2}}\big(\alpha|0_1\rangle + \beta|1_1\rangle\big)\big(|0_2 0_3\rangle + |1_2 1_3\rangle\big)\\ &\quad\xrightarrow{\text{CNOT}_{12}}\big(\alpha|0_1 0_2 0_3\rangle + \alpha|0_1 1_2 1_3\rangle + \beta|1_1 1_2 0_3\rangle + \beta|1_1 0_2 1_3\rangle\big)\\ &\quad\xrightarrow{\text{M}_2(|0_2\rangle)}\big(\alpha|0_1 0_3\rangle + \beta|1_1 1_3\rangle\big)|0_2\rangle\,.\end{aligned} \tag{60}$$

If the result of measuring M_2 is $|1_2\rangle$, the information about it is transmitted to point B via a classical channel and the $\text{X} = \text{NOT}$ operation is performed on qubit 3 there. This transformation has the result

$$\xrightarrow{\text{M}_2(|1_2\rangle)}\big(\alpha|0_1 0_3\rangle + \beta|1_1 1_3\rangle\big)|1_2\rangle\,.$$

With $|r_2\rangle$ denoting the state of qubit 2 upon the measurement, we write the qubit states at this stage:

$$|\psi\rangle = \big(\alpha|0_1 0_3\rangle + \beta|1_1 1_3\rangle\big)|r_2\rangle\,.$$

Qubits 1 and 3 have become entangled.

The measurement M_2 performed on qubit 2 has released it from entanglement. We use this property of measurement once more to release qubit 1 from entanglement,

$$\begin{aligned}&\big(\alpha|0_1 0_3\rangle + \beta|1_1 1_3\rangle\big)|r_2\rangle \xrightarrow{\text{H}_1}\big(\alpha|(+)_1 0_3\rangle + \beta|(-)_1 1_3\rangle\big)|r_2\rangle\\ &\quad\xrightarrow{\text{M}_1(|0_1\rangle)}\big(\alpha|0_3\rangle + \beta|1_3\rangle\big)|0_1\rangle|r_2\rangle\,,\end{aligned} \tag{61}$$

where $(\pm) = |0\rangle \pm |1\rangle$. If the result of measuring M_1 is $|1_1\rangle$, the classical information about that is transmitted to point B and operation Z is performed on qubit 3 there. The final state of the three qubits is

$$|\psi_{\text{f}}\rangle = \big(\alpha|0_3\rangle + \beta|1_3\rangle\big)|r_1\rangle|r_2\rangle\,. \tag{62}$$

What is the outcome of all operations? The unknown state $|a_1\rangle = \alpha|0_1\rangle + \beta|1_1\rangle$, which initially belonged to qubit 1 at point A, now belongs to qubit 3 at point B — the teleportation of the unknown state has occurred. Qubit 1 was deprived of the $|a_1\rangle$ state: its retention in qubit 1 would have implied the cloning of the unknown state, which is forbidden by the no-cloning theorem. The final state of the three qubits is not entangled. The entanglement produced at the beginning of the operation was expended on the performance of the teleportation. Formula (62) implies that entanglement is an expendable resource of quantum informatics.

A 'miracle' in this case is the teleportation of just the unknown quantum state. The teleportation of a known state can be realized without quantum entanglement, taking advantage of only the methods of classical physics. Let the state of qubit 1 be known: for instance, $|a_1\rangle = |0\rangle$. We transmit the information about the state of qubit 1 to point B. Employing the information obtained, the operator at point B brings qubit 3 to the state $|0\rangle$. Such is the teleportation scheme in the classical world: the complete information about

an object is transmitted from point A to point B, where the object is recreated.

6.3 Modeling of quantum systems with a quantum computer

We consider the problem of quantum computer-assisted simulation of a quantum system with the Hamiltonian

$$H = \frac{p^2}{2m} + V(x)\,.$$

The static problem consists in the determination of energy eigenvalues E and eigenfunctions $|u\rangle$ of the system, which obey the equation

$$H|u\rangle = E|u\rangle\,.$$

The dynamic problem involves the study of the dynamics of the system according to the Schrödinger equation

$$\mathrm{i}\,\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$$

(the constant $\hbar$ is included in the Hamiltonian H). Using the evolution operator $\mathrm{U}(t) = \exp(-\mathrm{i}Ht)$, the dynamic equation can be reduced to the transformation of the system state vector:

$$\big|\psi(x,t)\big\rangle = \mathrm{U}(t)\,\big|\psi(x,0)\big\rangle\,. \tag{63}$$

If the eigenvalue problem is solved, E and $|u\rangle$ are known and

$$\big|u(t)\big\rangle = \exp\left(-\mathrm{i}\,\frac{Et}{\hbar}\right)\big|u(0)\big\rangle\,.$$

Simulating a quantum system with a quantum computer requires 'inputting' the state vector (the wave function) of the system in the quantum register, which consists of qubits [15]. Let the function $\psi(x)$ be defined in the interval $-d \leqslant x \leqslant d$. We digitize the continuous variable x with an increment Δ:

$$x_k = k\Delta\,, \qquad -\frac{d}{\Delta} \leqslant k \leqslant \frac{d}{\Delta}\,.$$

The discrete state function $\big|\tilde{\psi}(x_k)\big\rangle$ defined at $2d/\Delta + 1$ points is a vector with $2d/\Delta + 1$ complex components, which can be identified with the components c_k of the state vector

$$|\psi\rangle = \sum_{k=0}^{2^n-1} c_k|k\rangle\,, \qquad n = \log_2\left(2\,\frac{d}{\Delta} + 1\right),$$

of the n-qubit register of the quantum computer. The accuracy of the $\big|\psi(x)\big\rangle$ representation depends on the number of qubits in the register: the discretization increment is exponentially small owing to the exponentially large number of dimensions of the state of the quantum register. Quantum systems with a discrete set of states are also easy to map onto the states of a qubit register.

We now turn to the problem of computing the eigenvalues E of the Hamiltonian of a quantum system using a quantum computer. The evolution operator $\mathrm{U} = \exp(-\mathrm{i}Ht)$ is a unitary operator, its eigenvalues $\big|\exp(\mathrm{i}\varphi)\big| = 1$, and therefore

$$\mathrm{U}|u\rangle = \exp(\mathrm{i}\varphi)\,|u\rangle\,. \tag{64}$$

Keeping the equality

$$\big\langle u\big|\exp(-\mathrm{i}Ht)\big|u\big\rangle = \exp(-\mathrm{i}\omega t)\,, \qquad E = \varphi\,\frac{\hbar}{t}$$

in mind, we consider the algorithm for the estimation of the phase φ of the quantum system with a quantum computer. We mark out two qubit registers in the computer:

$$|\psi_{\mathrm{in}}\rangle = |0\rangle|u\rangle\,.$$

All qubits of the first register are initialized (all in the $|0\rangle$ state); mapped onto the second register is the eigenstate $|u\rangle$ of the quantum system under investigation.

The next operation is the quantum Fourier transformation (QFT) of the state of the first register. The QFT is identical to the discrete Fourier transformation. The Fourier transform of an N-dimensional vector $(x_0, \ldots, x_{N-1})$ with complex components x_j is an N-dimensional complex vector $(y_0, \ldots, y_{N-1})$ with the components [15]

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(\mathrm{i}\,\frac{2\pi jk}{N}\right) x_j\,. \tag{65}$$

The QFT performed in quantum registers maps the state vector

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j|j\rangle$$

onto its Fourier transform

$$\mathrm{QFT}|\psi\rangle = \sum_{k=0}^{N-1} y_k|k\rangle\,,$$

where y_k are defined by equality (65). Upon substituting expression (65) for y_k in the right-hand side of $\mathrm{QFT}|\psi\rangle$, we obtain the expression for the QFT of the basis states:

$$\mathrm{QFT}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\mathrm{i}\,\frac{2\pi jk}{N}\right)|k\rangle\,, \qquad N = 2^n\,. \tag{66}$$

The phase $\varphi_{jk} = 2\pi jk/N$ of the term $|k\rangle$ is defined by the combination of the values of j and k of the basis states $|j\rangle$ and $|k\rangle$.

Upon defining QFT, we revert to our problem. We perform the QFT of the state $|0\rangle$ of the first register:

$$|0_1\rangle|u_2\rangle \xrightarrow{\mathrm{QFT}_1} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|u\rangle\,. \tag{67}$$

Sum (67) decomposes into the product of the superpositions $(1/\sqrt{2})\big(|0\rangle + |1\rangle\big)$ for each of n qubits of the first register:

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$
$$\equiv \frac{1}{\sqrt{2}}\big(|0_1\rangle + |1_1\rangle\big) \cdot \frac{1}{\sqrt{2}}\big(|0_2\rangle + |1_2\rangle\big) \cdot \ldots \cdot \frac{1}{\sqrt{2}}\big(|0_n\rangle + |1_n\rangle\big)\,. \tag{68}$$

Under the control of the qubits of the first register (of qubits $1, 2, \ldots, n$ sequentially), we apply the U operator to the second register $2^0, 2^2, \ldots, 2^{n-1}$ times, respectively. The

transformations

$$\mathrm{U}^{2^0}|u\rangle, \mathrm{U}^{2^2}|u\rangle, \ldots, \mathrm{U}^{2^{n-1}}|u\rangle$$

result in the occurrence of the phase factors

$$\exp(\mathrm{i}\varphi), \exp(2^2\mathrm{i}\varphi), \ldots, \exp(2^{n-1}\mathrm{i}\varphi),$$

at the states $|1\rangle$ of the controlling qubits:

$$\frac{1}{\sqrt{N}}\big(|0\rangle + \exp(2^{n-1}\cdot 2\pi\mathrm{i}\varphi)|1\rangle\big)\big(|0\rangle + \exp(2^{n-2}\cdot 2\pi\mathrm{i}\varphi)|1\rangle\big)$$
$$\ldots\big(|0\rangle + \exp(2^0\cdot 2\pi\mathrm{i}\varphi)|1\rangle\big) \equiv \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp(2\pi\mathrm{i}\varphi k)|k\rangle\,. \tag{69}$$

The inverse QFT of the first register brings it back to the state $|\varphi\rangle$. Performing the state measurement of the first register, we obtain the value of the sought phase φ in the n-qubit representation.

In the foregoing, the eigenfunction $|u\rangle$ of the operator U was assumed to be known. However, in practice, we may have some approximation of $|u\rangle$ obtained, for instance, from approximate calculations with a classical computer. This approximation is referred to as the trial function $|u_{\mathrm{p}}\rangle$. When the approximation $|u_{\mathrm{p}}\rangle$ is not too bad, the product $\langle u_{\mathrm{p}}|u\rangle$ is not exponentially small.

We repeat the computations to estimate the phase, introducing $|u_{\mathrm{p}}\rangle$ in the second register instead of $|u\rangle$. If $|u_{\mathrm{p}}\rangle$ is decomposed in terms of $|u\rangle$,

$$|u_{\mathrm{p}}\rangle = \sum_s c_s|u_s\rangle\,,$$

all computations performed above can be repeated without changes. The state of the second register is the only change: the superposition $\sum_s c_s|u_s\rangle$ is in place of $|u_s\rangle$. Upon measuring the state of the second register, we arrive at the solution $|u_s\rangle$ with the probability $|c_s|^2$ [39].

6.4 Modeling of quantum systems dynamics with a quantum computer

The quantum dynamics of a system can be represented as the transformation of the initial state vector $\big|\psi(x,0)\big\rangle$ by the quantum evolution operator $\mathrm{U} = \exp(-\mathrm{i}Ht)$:

$$\big|\psi(x,t)\big\rangle = \exp(-\mathrm{i}Ht)\big|\psi(x,0)\big\rangle\,. \tag{70}$$

The first problem that emerges in this transformation is the occurrence of noncommuting parts; for instance, for a one-dimensional particle motion,

$$H = H_0 + H_1\,, \qquad H_0 = \frac{p^2}{2m}\,, \qquad H_1 = V(x)\,,$$

the operators of kinetic and potential particle energy do not commute.

To represent the evolution operator as the product of evolution operators, one of the approximations [15]

$$\exp\big(\mathrm{i}(A+B)\,\Delta t\big) = \exp(\mathrm{i}A\,\Delta t)\exp(\mathrm{i}B\,\Delta t) + O(\Delta t^2)\,, \tag{71}$$

$$\exp\big(\mathrm{i}(A+B)\,\Delta t\big) = \exp(\mathrm{i}A\,\Delta t)\exp(\mathrm{i}B\,\Delta t)\times$$
$$\times\exp\left(-\frac{1}{2}[A,B]\,\Delta t^2\right) + O(\Delta t^3)\,, \tag{72}$$

$$\exp\big(\mathrm{i}(A+B)t\big) = \lim_{n\to\infty}\left(\exp\left(\mathrm{i}\,\frac{At}{n}\right)\exp\left(\mathrm{i}\,\frac{Bt}{n}\right)\right)^n \tag{73}$$

can be used. In our example of one-dimensional particle motion, recourse can be made to approximation (71).

7. Processes that decohere qubit states and quantum computers

7.1 Decohering of quantum system states

In the theory of an ideal quantum computer outlined above, it was assumed that the quantum superpositions $|\psi\rangle = \sum c_x|x\rangle$ that describe the L-qubit register state remain coherent for an arbitrarily long time in the course of computation. However, the interaction of the register with the uncontrollable environment, the inaccuracy of the parameter values of control pulses, and the uncontrollable interqubit interaction are the source of decoherence of the quantum state $|\psi\rangle = \sum_x c_x|x\rangle$. Decoherence implies that a coherent state of the system transforms into a mixed one, which is described by the density matrix

$$\rho = \sum_x |c_x|^2|x\rangle\langle x|\,.$$

The description of a system by a density matrix does not contain information about the phases of the basis states, which deprives the system of the capacity to interfere and become entangled. The decohering of the state of the quantum system actually signifies its classicization, i.e., transition to a state described by classical physical laws.

An important parameter of a quantum system is the time of decohering τ_{dc} of its states. Below, we consider τ_{dc} for a single qubit and τ_{dc}^L for a register of L qubits. We show that the register of L qubits loses its state coherence in a shorter time:

$$\tau_{\mathrm{dc}}^L = \frac{\tau_{\mathrm{dc}}}{L^\alpha}\,, \qquad \alpha = 1, 2\,.$$

The decoherence time should be compared with the mean time τ_{op} taken to perform a computational operation: the ratio $N_{\mathrm{op}} = \tau_{\mathrm{dc}}^L/\tau_{\mathrm{op}}$ shows how many computational operations can be performed while the quantum computer retains its state coherence. In view of the relation $\tau_{\mathrm{dc}}^L = \tau_{\mathrm{dc}}/L^\alpha$, we have

$$N_{\mathrm{op}} = \frac{\tau_{\mathrm{dc}}}{\tau_{\mathrm{op}}L^\alpha}\,. \tag{74}$$

The values of τ_{dc} and τ_{op} may vary widely for different qubit realizations, but their ratio depends only slightly on the realization, $\tau_{\mathrm{dc}}/\tau_{\mathrm{op}} = 10^3 - 10^6$.

From formula (74), it follows that it is possible to perform only a small number of computational operations with a computer containing $L = 10^3$ qubits. For instance, Shor's algorithm for L-digit number factorization requires L^3 operations. The requisite duration of computation exceeds the computer coherence time by many orders of magnitude:

$$\frac{\tau_{\mathrm{Shor}}}{\tau_{\mathrm{dc}}^L} = \frac{\tau_{\mathrm{op}}L^3}{\tau_{\mathrm{dc}}/L^\alpha} = \frac{\tau_{\mathrm{op}}}{\tau_{\mathrm{dc}}}\,L^{(3+\alpha)}\,. \tag{75}$$

For $L = 10^3$, $\tau_{\mathrm{op}}/\tau_{\mathrm{dc}} = 10^{-5}$, and $\alpha = 1$, we obtain $\tau_{\mathrm{Shor}}/\tau_{\mathrm{dc}}^L \simeq 10^7$.

The above estimates imply that the processes of decohering of quantum computer states 'prohibit' the existence of a full-scale (i.e., capable of solving big problems) quantum computer. Is there a way out? There are obvious proposals

that follow from formula (75): (1) it is necessary to shorten the time of operation $\tau_{\rm op}$; (2) it is necessary to lengthen the qubit decoherence time $\tau_{\rm dc}$.

The time $\tau_{\rm op}$ can be shortened by increasing the intensity of control fields. However, the control field intensities are bounded from above by the excitation of nonresonance transitions and the occurrence of other nonlinear effects. Increasing the time $\tau_{\rm dc}$ calls for a careful examination of all possible qubit decohering mechanisms in a given specific realization and for the development of specific measures to isolate qubits from the environment, increase the accuracy of control signals, etc.

However, all these measures may prove to be insufficient to afford the requisite computation time. What needs to be devised is a way of stabilizing the coherent computer state for an arbitrarily long time in order to be able to complete the solution of any problem with a 'long' (though polynomially long) computation algorithm. This way is the method of quantum error correction.

The method involves a periodic 'cleaning' of a quantum computer's state of minor errors that emerge in the state vector due to decohering processes after the last cleaning. Also proposed are 'active' methods for the suppression of the decohering processes. But as regards the feasibility of a full-scale quantum computer operating in the coherent state for an arbitrarily long time, researchers are pinning their fervent hopes on the quantum method of error correction. The subsequent sections of this review are concerned with the decohering processes and the methods for error correction.

Investigations into the decoherence of quantum systems are a natural development of investigations of relaxation processes in many-particle systems, which were actively pursued throughout the XXth century. Spin–spin and spin–lattice relaxation processes actually coincide with the phase and amplitude decohering of spin qubits. Physicists acquainted with the literature on relaxation processes will encounter many familiar elements in decoherence theory. The decohering may be treated as the relaxation of coherence: in the course of decohering, the system goes from a non-equilibrium (coherent) state to an equilibrium (mixed) state; the process is accompanied by an increase in system entropy.

The processes of decohering of quantum systems are investigated in different models and approximations. The model whereby the environment of the system (a qubit, register) is described in a quantum way is the most adequate: decoherence arises as the result of entanglement of the system states with the states of the environment. In simpler models, the environment is described as fluctuating classical fields. The entanglement with the environment does not arise in these models explicitly, but the simplification of the description of the environment makes it possible to describe the decohering during quantum computations (operations) [40].

7.2 Phase decohering of a qubit

The elements of the quantum decoherence theory are revealed in the consideration of the simplest system consisting of two qubits: qubit q — a quantum system and qubit e — the quantum environment of the system. Let qubit q in the superposition state $|\psi\rangle = \alpha|0_q\rangle + \beta|1_q\rangle$ interact with the environment e in the state $|0_e\rangle$ to become entangled as a result of the CNOT_{qe} operation:

$$\big(\alpha|0_q\rangle + \beta|1_q\rangle\big)|0_e\rangle \xrightarrow{\mathrm{CNOT}_{qe}} \alpha|0_q\rangle|0_e\rangle + \beta|1_q\rangle|1_e\rangle \equiv |\psi_{qe}\rangle\,. \quad (76)$$

We calculate the reduced density matrix of qubit q (the quantum system) by averaging ρ_{qe} over the state of the environment:

$$\rho_q = \langle 0_e|\rho_{qe}|0_e\rangle + \langle 1_e|\rho_{qe}|1_e\rangle = |\alpha|^2|0_q\rangle\langle 0_q| + |\beta|^2|1_q\rangle\langle 1_q|\,. \quad (77)$$

The entanglement with the orthonormal states of the environment has led to the complete decoherence of the qubit system: its state is now described by a diagonal density matrix; the nondiagonal (coherence) elements are equal to zero. Although the $|\psi_{qe}\rangle$ state of the system qe in expression (76) is coherent, the subsystem q is in a mixed state. In the simplified treatment outlined above, decoherence emerges more or less abruptly; the description of the decoherence as a process is absent. In reality, the process is concealed inside the CNOT_{qe} operation performed in a finite time during which qubits q and e interact. When the CNOT_{qe} operation is completed, the decohering of qubit q is also completed.

We now somewhat augment the model of the decohering of qubit q in the quantum environment e. Initially, at $t = 0$, qubit q and the environment e are not entangled:

$$\big|\psi_{qe}(0)\big\rangle = \big(\alpha|0_q\rangle + \beta|1_q\rangle\big)\big|e(0)\big\rangle\,.$$

Let the interaction be turned on. After a lapse of time t, the qubit and the environment are entangled:

$$\big|\psi_{qe}(t)\big\rangle = \alpha|0_q\rangle\big|e_0(t)\big\rangle + \beta|1_q\rangle\big|e_1(t)\big\rangle\,.$$

If $t < t_{\rm dc}$, the states $\big|e_0(t)\big\rangle$ and $\big|e_1(t)\big\rangle$ are normalized but not orthogonal:

$$\big\langle e_0(t)\big|e_0(t)\big\rangle = \big\langle e_1(t)\big|e_1(t)\big\rangle = 1\,, \qquad \big\langle e_0(t)\big|e_1(t)\big\rangle = \cos\theta\,.$$

The 'angle' θ between the state vectors of the environment characterizes the decohering. For $t = 0$, the environment states are $\big|e_0(0)\big\rangle = \big|e_1(0)\big\rangle = \big|e(0)\big\rangle$, with $\big\langle e_0(0)\big|e_1(0)\big\rangle = 1$. During decohering, $\cos\theta \to 0$ and $\theta \to \pi/2$, i.e., the vectors $\big|e_0(t)\big\rangle$ and $\big|e_1(t)\big\rangle$ are orthogonalized.

We introduce a vector $|e_0^{\perp}(t)\rangle$ orthogonal to $|e_0(t)\rangle$; we select the vectors $|e_0(t)\rangle$ and $|e_0^{\perp}(t)\rangle$ as the basis. If $\langle e_0(t)|e_1(t)\rangle = \cos\theta$, then $\langle e_0^{\perp}(t)|e_1(t)\rangle = \sin\theta$. Representing the density matrix of the system and the environment as $\rho_{qe}(t) = \big|\psi_{qe}(t)\big\rangle\big\langle\psi_{qe}(t)\big|$, we use the formula

$$\rho_q(t) = \big\langle e_0(t)\big|\rho_{qe}\big|e_0(t)\big\rangle + \big\langle e_0^{\perp}(t)\big|\rho_{qe}\big|e_0^{\perp}(t)\big\rangle$$

to find the reduced density matrix of the qubit,

$$\rho_q(t) = |\alpha|^2|0_q\rangle\langle 0_q| + \alpha\beta^*|1_q\rangle\langle 0_q|\cos\theta + \alpha^*\beta|0_q\rangle\langle 1_q|\cos\theta + |\beta|^2|1_q\rangle\langle 1_q|\,,$$

or in the matrix form,

$$\rho_q(t) = \begin{pmatrix} |\alpha|^2 & \alpha\beta^*\cos\theta(t) \\ \alpha^*\beta\cos\theta(t) & |\beta|^2 \end{pmatrix}. \quad (78)$$

The nondiagonal matrix elements of the reduced density matrix are termed the coherences. With time, $\cos\theta(t) \to 0$ and the coherences vanish. The term 'decohering' acquires literal sense: this process consists of the disappearance of the coherences in the density matrix of the qubit. Another feature

of the process described by density matrix (78) is the invariance of the moduli α and β of the amplitudes; only their phases change. Matrix (78) therefore describes the so-called phase decohering of the qubit.

7.3 Operator of qubit decohering

In the model of decohering of qubit q in the quantum environment e, it is also possible to include the amplitude decohering by obtaining the combined description of the processes of phase and amplitude decohering, which proceed simultaneously:

$$\begin{aligned}\big|\psi_{qe}(0)\big\rangle &= \big(\alpha|0\rangle + \beta|1\rangle\big)|e\rangle \\ &\xrightarrow{\mathrm{dc}} \alpha|0\rangle|e_{00}\rangle + \alpha|1\rangle|e_{01}\rangle + \beta|1\rangle|e_{11}\rangle + \beta|0\rangle|e_{10}\rangle\,. \qquad (79)\end{aligned}$$

The amplitude $|e_{01}\rangle$ describes the transition from the qubit state $\alpha|0\rangle$ to the state $|1\rangle$; this decreases the initial amplitude α of the state $|0\rangle$ to the value $\alpha|e_{00}\rangle$. The significance of the amplitudes $\beta|e_{10}\rangle$ and $\beta|e_{11}\rangle$ is precisely the same.

We write transformation (79) in the matrix form:

$$\begin{vmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{vmatrix} \to \begin{pmatrix}|e_{00}\rangle & |e_{01}\rangle\\ |e_{10}\rangle & |e_{11}\rangle\end{pmatrix}\begin{vmatrix}\alpha|0\rangle\\ \beta|1\rangle\end{vmatrix}. \qquad (80)$$

The decomposition of the matrix of decohering ($|e_{ij}\rangle$) in terms of the Pauli matrices σ_i is referred to as the operator of decohering E:

$$\mathrm{E} = \begin{pmatrix}|e_{00}\rangle & |e_{01}\rangle\\ |e_{10}\rangle & |e_{11}\rangle\end{pmatrix} \equiv |e_0\rangle\sigma_0 + |e_1\rangle\sigma_x + \mathrm{i}|e_2\rangle\sigma_y + |e_3\rangle\sigma_z\,, \qquad (81)$$

$$|e_{0,1}\rangle = \frac{1}{2}\big(|e_{00}\rangle \pm |e_{11}\rangle\big)\,, \qquad |e_{2,3}\rangle = \frac{1}{2}\big(|e_{01}\rangle \pm |e_{10}\rangle\big)\,. \qquad (82)$$

The transformation

$$\mathrm{E}|\psi\rangle|e\rangle = \sum_{j=0}^{3}|e_j\rangle\sigma_j|\psi\rangle \qquad (83)$$

describes the decohering in the generalized form as the sum of the following operations: undo (identical transformation σ_0), qubit flipping ($\sigma_x = \mathrm{NOT}$, $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$), phase change (σ_z, $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$), and flip with a phase change ($\mathrm{i}\sigma_y$).

How strongly the decohered state

$$\big|\psi(t)\big\rangle = \sum_{j=0}^{3}|e_j\rangle\sigma_j\big|\psi(0)\big\rangle$$

differs from the initial state $\big|\psi(0)\big\rangle$ is characterized by the fidelity parameter

$$\begin{aligned}F_\psi(t) &= \big\langle\psi(0)\big|\psi(t)\big\rangle\big\langle\psi(t)\big|\psi(0)\big\rangle \\ &= \sum_{i,j}\big\langle\psi(0)\big|\sigma_j\big|\psi(0)\big\rangle\big\langle\psi(0)\big|\sigma_i\big|\psi(0)\big\rangle\big\langle e_j(t)\big|e_i(t)\big\rangle\,. \qquad (84)\end{aligned}$$

The parameter $F_\psi(t)$ depends on the initial state $\big|\psi(0)\big\rangle$, which is marked with the subscript ψ. More representative values of $F(t)$ are obtained on averaging over some set of states ψ_s:

$$\tilde{F}(t) = \frac{1}{n}\sum_{s=1}^{n}F_{\psi_s}(t)\,. \qquad (85)$$

The notions and operators introduced above are easily generalized to the case of n qubits (a quantum computer). The parameters that characterize the time of decohering (the decoherence rate $\gamma = \tau_{\mathrm{dc}}^{-1}$) should be obtained either from experiment or by calculations on the basis of microscopic models. An example of such a calculation is provided in Section 7.4.

7.4 Microscopic theory of amplitude decohering

A clear and complete description of amplitude decohering may be obtained by solving the Schrödinger equation

$$\mathrm{i}\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$$

for a system with the Hamiltonian $H = H_q + H_e + H_{qe}$. Here, the Hamiltonian $H_q = \hbar\omega_0|1\rangle\langle 1|$ describes a qubit with energy levels $E_0 = 0$ and $E_1 = \hbar\omega_0$, $H_e = \sum_m \hbar\omega_m a_m^* a_m$ is the Hamiltonian of the system of surrounding oscillators, and the interaction Hamiltonian

$$H_{qe} = \sum_m \lambda_m|0\rangle\langle 1|a_m^* + \lambda_m^*|1\rangle\langle 0|a_m$$

describes the transitions with an energy exchange between the qubit and the environment:

$$|0\rangle|n_m\rangle \to |1\rangle|n_m - 1\rangle\,, \qquad |1\rangle|n_m - 1\rangle \to |0\rangle|n_m\rangle\,.$$

We specify the initial conditions: for $t = 0$, the qubit is in the state $|1_q\rangle$, i.e., $c_1(0) = 1$, and the oscillators of the environment are in the vacuum state $|0_1 \ldots 0_l \ldots 0_m\rangle$. Due to the interaction H_{qe}, for $t > 0$, there emerges the state

$$|\psi_l\rangle = |0_q\rangle|0_1 \ldots 1_l \ldots 0_m\rangle\,, \qquad l = 1, \ldots, m\,,$$

with a nonzero amplitude $c_l(t)$.

The desired solution is an entangled state of the qubit and the environment:

$$\big|\psi(t)\big\rangle = c_1(t)\exp(\mathrm{i}\omega_0 t)|\psi_1\rangle + \sum_{l=1}^{m}c_l(t)\exp(\mathrm{i}\omega_l t)|\psi_l\rangle\,, \qquad (86)$$

$$c_1(0) = 1\,, \qquad c_l(0) = 0\,.$$

We perform conventional calculations to obtain the equations for the amplitudes $c_1(t)$ and $c_l(t)$ from the Schrödinger equation,

$$\mathrm{i}\hbar\dot{c}_1 = \sum_{l=1}^{m}\lambda_l^* c_l\exp\big(-\mathrm{i}(\omega_l - \omega_0)t\big)\,, \qquad (87)$$

$$\mathrm{i}\hbar\dot{c}_l = \lambda_l c_1\exp\big(\mathrm{i}(\omega_l - \omega_0)t\big)\,. \qquad (88)$$

Eliminating $c_l(t)$ from Eqn (87), we obtain the equation for $c_1(t)$:

$$\dot{c}_1(t) = \int_0^t c_1(t')\,k(t - t')\,\mathrm{d}t'\,, \qquad (89)$$

where

$$k(t - t') = \frac{1}{\hbar^2}\sum_{l=1}^{m}|\lambda_l|^2\exp\big(-\mathrm{i}(\omega_l - \omega_0)(t - t')\big)\,. \qquad (90)$$

For the times $t \leqslant 2\pi/(\omega_l - \omega_0)$ such that

$$\exp\big(-\mathrm{i}(\omega_l - \omega_0)t\big) \simeq 1$$

and assuming that $c_1(t') = c_1(0) = 1$, we have

$$\left|c_1(t)\right|^2 = 1 - \frac{1}{\hbar^2}\sum_{l=1}^{m}|\lambda_l|^2 t^2\,, \qquad t^2 \ll \hbar^2\left(\sum_{l=1}^{m}|\lambda_l|^2\right)^{-1}. \quad (91)$$

The result (91) is interesting from the physical standpoint: initially, the amplitude of the initial state decreases only quadratically in the small quantity t^2. In what follows, we use this result in the interpretation of the so-called quantum Zeno effect.

We rewrite relation (89) as

$$\dot{c}_1(t) \simeq -c_1(t)\Gamma(t)\,, \qquad \Gamma(t) = \int_0^t k(\tau)\,\mathrm{d}\tau\,. \quad (92)$$

The main contribution to the integral $\Gamma(t)$ is made by the term $\omega_l = \omega_0$. This allows the integration with respect to τ to be extended to ∞, with the result (see Ref. [41])

$$\frac{\gamma}{2} \equiv \Gamma(\infty) = \frac{2\pi}{\hbar^2}\left|\lambda(\omega_0)\right|^2, \quad (93)$$

$$c_1(t) = \exp\left(-\frac{\gamma}{2}\,t\right), \quad (94)$$

$$c_l(t) = \frac{\lambda_l}{\hbar}\,\frac{1-\exp\left(\mathrm{i}(\omega_l - \omega_0' + \mathrm{i}\gamma/2)t\right)}{\omega_l - \omega_0' + \mathrm{i}\gamma/2}\,, \quad (95)$$

where

$$\omega_0' = \omega_0 + \delta\,, \qquad \delta = P\sum_{l=1}^{m}\frac{|\lambda_l|^2}{\omega_0 - \omega_l}\,.$$

7.5 Phase and amplitude decohering of a spin qubit in a random classical field

For a spin qubit — a spin $S = 1/2$ particle in a constant external magnetic field $\mathbf{B}(0,0,B_z)$ — the solution of the Schrödinger equation subjected to the initial conditions $\left|\psi(0)\right\rangle = \alpha|0\rangle + \beta|1\rangle$ has the form

$$\left|\psi(t)\right\rangle = \exp\left(\frac{\mathrm{i}}{\hbar}\,H_0 t\right)\left|\psi(0)\right\rangle$$

$$= \exp\left(\frac{\mathrm{i}}{\hbar}\,E_0 t\right)\left[\alpha|0\rangle + \beta\exp\left(\frac{\mathrm{i}}{\hbar}(E_1 - E_0)t\right)|1\rangle\right], \quad (96)$$

where $E_0 = -\hbar\omega/2$ and $E_1 = \hbar\omega/2$ are the spin energy levels that correspond to the states $|0\rangle$ and $|1\rangle$ of the spin qubit.

Under conditions of magnetic resonance in liquids, added to the constant field $\mathbf{B}(0,0,B_z)$ is the random internal magnetic field $\Delta\mathbf{B}(\Delta\mathbf{B}_\perp, \Delta B_z)$ produced, for instance, by the spins of all other particles surrounding the spin qubit. The Brownian motion of particles in the system (translational and rotational diffusion) makes $\Delta\mathbf{B}$ a random function of time with the correlation time τ_c.

The longitudinal component of the random field ΔB_z makes a contribution $\Delta E = g\beta\,\Delta B_z$ to the difference between the energy levels of the spin qubit and a random phase increment $\Delta\varphi(t) = \Delta E t$. The random phase increments $\Delta\varphi(t)$ are responsible for the phase decohering of the spin qubit. Similarly, the transverse component of the random field $\mathbf{B}_\perp(t)$ is responsible for the amplitude (dissipative) decohering of the spin qubit. The above model furnishes a simple description of these important processes.

The random process $\Delta\varphi(t) = \Delta\omega(t)\,t$ may be represented as a stepwise process with a characteristic time interval τ_c,

$$\Delta\varphi_i(\tau_c) = \Delta\omega_i\,\tau_c\,, \qquad i = 1,\ldots,n\,,$$

where $\Delta\omega_i$ is the frequency shift of the qubit resonance constant during the time τ_c. Then,

$$\Delta\varphi(t) = \Delta\varphi(n\tau_c) = \sum_{i=1}^{n}\Delta\varphi_i = \left(\sum_{i=1}^{n}\Delta\omega_i\right)\tau_c\,.$$

For an alternating process,

$$\sum_i \Delta\varphi_i = 0\,, \qquad \sum_i \Delta\omega_i = 0\,,$$

but $\overline{\Delta\varphi^2} = \tau_c^2 n\,\overline{\Delta\omega_i^2} \equiv \overline{\Delta\omega_i^2}\,\tau_c t$. The bar denotes averaging:

$$\overline{\Delta\omega_i^2} = \frac{1}{n}\sum_{i=1}^{n}\omega_i^2\,.$$

The root-mean-square qubit phase increment is proportional to the duration of the random process.

We define the qubit phase decoherence time $t_{\mathrm{dc,ph}}$ as the time taken to reach $\overline{\Delta\varphi^2} = 1$ rad^2. Then, from the equality $\overline{\Delta\varphi^2} = \overline{\Delta\omega_i^2}\,\tau_c t_{\mathrm{dc,ph}} = 1$, we obtain the phase decoherence time:

$$t_{\mathrm{dc,ph}} = \frac{1}{\overline{\Delta\omega^2}\,\tau_c}\,. \quad (97)$$

If $\overline{\Delta\omega^2}$ is determined by the dipole–dipole interaction of similar spins separated by a distance r, we have

$$\overline{\Delta\omega^2} = \frac{3}{2}\,\frac{\mu^4}{\hbar^2 r^6} \equiv \frac{3}{2}\,\frac{\gamma^4\hbar^2}{r^6}\,.$$

This formula and relation (97) imply that

$$\frac{1}{t_{\mathrm{dc,ph}}} = \frac{3}{2}\,\frac{\gamma^4\hbar^2}{r^6}\,\tau_c\,.$$

For nuclear spins in molecular liquids, the values $t_{\mathrm{dc,ph}} \simeq 1$ s.

We now consider the amplitude qubit decohering in the model of random fields. In the state $|\psi\rangle = \alpha|0\rangle + \exp(\mathrm{i}\varphi)\,\beta|1\rangle$, the magnetization of the spin qubit is

$$M_z = \gamma\hbar\sum_{S_z=-1/2}^{+1/2} p_{S_z} S_z = \frac{1}{2}\,\gamma\hbar\left(|\beta|^2 - |\alpha|^2\right). \quad (98)$$

It follows from (98) that any process that changes the magnetization M_z is an amplitude process, changing the amplitudes $|\alpha|$ and $|\beta|$.

We show that the occurrence of the transverse random magnetic field $\Delta\mathbf{B}_\perp$ is responsible for random increments of the magnetization $M_z(t)$ and hence for random changes of the amplitudes.

We introduce two coordinate systems: Oxz with the z axis aligned with the constant field $\mathbf{B}$ and $Ox'z'$ with the z' axis aligned with the field $\mathbf{B} + \Delta\mathbf{B}_\perp$ (Fig. 10). The angle θ between the axes Oz and Oz' is determined by $\tan\theta = \Delta B_\perp/B \ll 1$. At the time instant $t = 0$, the projections of the magnetization on the axes Oz' and Ox' are defined as

$$M_{z'}(0) = M_z(0)\cos\theta\,, \qquad M_{x'}(0) = -M_z(0)\sin\theta\,. \quad (99)$$

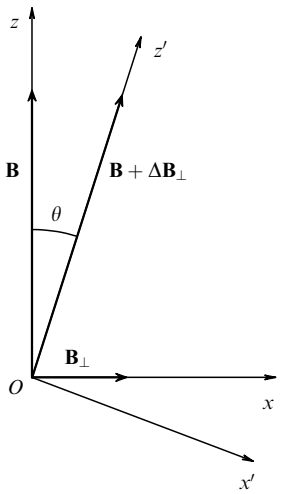

Figure 10. Coordinate systems associated with the external constant ($\mathbf{B}$) and total ($\mathbf{B}+\Delta\mathbf{B}_\perp$) fields.

At the time instant $t=\tau_c$, these projections are given by

$$M_{z'}(\tau_c)=M_z(0)\cos\theta\,,\qquad M_{x'}(\tau_c)=-M_z(0)\cos(\omega_0\tau_c)\sin\theta\,. \tag{100}$$

The factor $\cos(\omega_0\tau_c)$ is due to the precession of $M_{x'}$ about the axis Oz' with the frequency ω_0. For the time τ_c, the random field $\Delta\mathbf{B}_\perp$ is assumed to be constant (a stepwise process).

We determine $M_z(\tau_c)$:

$$M_z(\tau_c)=M_{z'}(\tau_c)\cos\theta-M_{x'}(\tau_c)\sin\theta = M_z(0)\left[1-\sin^2\theta\left(1-\cos(\omega_0\tau_c)\right)\right]. \tag{101}$$

We assume that $\omega_0\tau_c\ll 1$ and express $\sin\theta$ in (101) from $\tan\theta=\Delta B_\perp/B$, with the result

$$\frac{M_z(\tau_c)}{M_z(0)}=1-\frac{\Delta B_\perp^2}{B^2}\,\frac{\omega_0^2\tau_c^2}{2}\,. \tag{102}$$

Formula (102) implies an equation for the relaxation of the longitudinal magnetization M_z (the amplitudes $|\alpha|$ and $|\beta|$),

$$\frac{M_z(\tau_c)-M_z(0)}{\tau_c M_z(0)}=\frac{\mathrm{d}}{\mathrm{d}t}\,\frac{M_z}{M_z(0)}=-\frac{1}{t_{M_z}}=-\frac{\Delta B_\perp^2\gamma^2\tau_c}{2}\,. \tag{103}$$

The relaxation process for the longitudinal spin magnetization

$$M_z(t)=M_z(0)\exp\left(-\frac{t}{t_{M_z}}\right)+M_z^{\mathrm{B}}\,, \tag{104}$$

leads to the value of magnetization M_z^{B} for the Boltzmann population distribution of qubit energy levels. The relaxation time of the longitudinal spin magnetization is simultaneously the time of amplitude qubit decohering:

$$t_{\mathrm{dc,amp}}=t_{M_z}=\frac{2}{\Delta B_\perp^2\gamma^2\tau_c}\,.$$

For the dipole – dipole interaction of two similar spins separated by a distance r, we have

$$\frac{1}{t_{\mathrm{dc,amp}}}=\frac{3}{2}\,\frac{\gamma^4\hbar^2}{r^6}\,\tau_c\,.$$

In low-viscosity liquids, the times $t_{\mathrm{dc,amp}}$ and $t_{\mathrm{dc,ph}}$ coincide [42].

7.6 Decohering due to interqubit interactions: quantum chaos

From the standpoint of quantum computer operation, the situation where the interaction between a pair of qubits i and j is turned on only at the instant of performance of a two-qubit operation of the type

$$(\mathrm{Control})_{ij}-\mathrm{U}_{ij}$$

would be ideal; for the rest of the time, the interqubit interaction is absent. In real situations, some residual interaction H_{ij} between the qubits i and j always exists, i.e., during the execution of single-qubit operations and the free evolution (standing idle) of the computer.

As shown in Section 7.4, if we mark out one qubit and consider its decohering due to its interaction with another one, this process is similar to the qubit decohering due to its interaction with the quantum environment. Here, we consider the dynamics of a quantum computer consisting of a large number of interacting qubits [43]:

$$H=\sum_{i=1}^{n}\omega_i\sigma_z^{(i)}+\sum_{i<j}J_{ij}\sigma_x^{(i)}\sigma_x^{(j)}\,. \tag{105}$$

The resonance qubit frequencies ω_i and the interaction parameter J_{ij} are evenly distributed over the respective intervals $[0.5\Delta_0,\,1.5\Delta_0]$ and $[-J,\,J]$. The average spacing of computer energy levels is $\Delta_n=n\Delta_0/2^n$, where 2^n is the number of basis states of an n-qubit computer. The average spacing Δ_n is exponentially small, $\Delta_n\ll J$. Strong interqubit interactions in the computer correspond to the condition

$$\frac{J}{\Delta_0/n}>1\,.$$

In this case, computer simulation reveals the chaotic dynamics of the quantum computer.

For low interaction energies,

$$\frac{J}{\Delta_0/n}\ll 1\,,$$

a deterministic computer dynamics is observed. For deterministic dynamics, the state vector contains a small number of basis functions. For chaotic dynamics, the superposition consists of a large number of basis states with small weights. In going over from a system with deterministic dynamics to a system with chaotic dynamics, the statistics of the intervals s between the system energy levels changes: a transition from the Poisson distribution

$$P_{\mathrm{P}}(s)=\exp(-s)$$

to the Wigner – Dyson distribution

$$P_{\mathrm{WD}}=\frac{\pi s}{2}\exp\left(-\frac{\pi s^2}{4}\right)$$

occurs.

The results of the theory of quantum chaos allow estimating the proposed realizations of a quantum computer from the standpoint of their remoteness from quantum chaos. To ensure that quantum chaotic dynamics does not emerge in

the computer, the interqubit interaction J should be weaker than the threshold value J_c [43]:

$$J \ll J_c = \frac{\Delta_0}{n} .$$

7.7 Decohering due to qubit control errors

The Hamiltonian of a qubit controlled by an external classical field $\mathbf{h}(t)$ can be written as

$$H(t) = \omega_0 \sigma_z + \boldsymbol{\sigma}\big(\mathbf{h}(t) + \delta\mathbf{h}(t)\big) , \tag{106}$$

where $\mathbf{h}(t)$ is the part of the control field that furnishes the desired ideal control and $\delta\mathbf{h}(t)$ is the control error caused by the fact that the field is controlled with some experimental inaccuracy $\delta h/h$. Control errors are treated as yet another source of errors in quantum computations along with the interaction of qubits with the environment and with each other.

We estimate the effect of control errors with the aid of the quantum computation fidelity parameter. In the cases of the ideal and real computation control, the final computer states are given by

$$\big|\psi^{(\mathrm{id})}(t)\big\rangle = \mathrm{U}^{(\mathrm{id})}\big|\psi(0)\big\rangle , \tag{107}$$

$$\big|\psi^{(\mathrm{re})}(t)\big\rangle = \mathrm{U}^{(\mathrm{re})}\big|\psi(0)\big\rangle . \tag{108}$$

The projections of $\big|\psi(t)\big\rangle$ on the basis states of the quantum computer are defined by the equalities

$$c_x^{(\mathrm{id})} = \big\langle x\big|\psi^{(\mathrm{id})}(t)\big\rangle , \qquad c_x^{(\mathrm{re})} = \big\langle x\big|\psi^{(\mathrm{re})}(t)\big\rangle . \tag{109}$$

From the normalization condition, we have

$$\sum_x \big|c_x^{(\mathrm{id})}\big|^2 = \sum_x \big|c_x^{(\mathrm{re})}\big|^2 = 1 .$$

For the criterion of quantum computation accuracy, we select the averaged norm of the scalar product of 2^L-dimensional vectors $c_x^{(\mathrm{id})}$ and $c_x^{(\mathrm{re})}$:

$$F = \left\langle \left| \sum_{x=0}^{2^L-1} c_x^{(\mathrm{id})} c_x^{(\mathrm{re})*} \right|^2 \right\rangle = \left\langle \left| \big\langle \mathrm{U}^{(\mathrm{id})}\psi(0)\big|\psi^*(0)\mathrm{U}^{(\mathrm{re})*}\big\rangle \right|^2 \right\rangle . \tag{110}$$

The exterior averaging is performed over the distribution of random increments that differentiate $c_x^{(\mathrm{re})}$ from $c_x^{(\mathrm{id})}$. If the computation is perfect, $c_x^{(\mathrm{re})} = c_x^{(\mathrm{id})}$ and $F = 1$.

We represent $\mathrm{U}^{(\mathrm{re})}$ as the ordered product of M matrices, $\mathrm{U}^{(\mathrm{re})} = \mathrm{U}_1^{(\mathrm{re})} \ldots \mathrm{U}_M^{(\mathrm{re})}$, each of which contains errors ξ_k and Φ_k:

$$\mathrm{U}_k^{(\mathrm{re})} = \\ = \begin{pmatrix} \cos(\theta_k + \xi_k) & \exp\big(\mathrm{i}(\varphi_k + \Phi_k)\big)\sin(\theta_k + \xi_k) \\ -\mathrm{i}\exp\big(-\mathrm{i}(\varphi_k + \Phi_k)\big)\sin(\theta_k + \xi_k) & \cos(\theta_k + \xi_k) \end{pmatrix} . \tag{111}$$

Expanding $\mathrm{U}_k^{(\mathrm{re})}$ in terms of the small increments ξ_k and Φ_k, we obtain

$$F = 1 - \left\langle \sum_{k=1}^{M} \big[c_k^{(\xi\xi)}\xi_k^2 + c_k^{(\xi\Phi)}\xi_k\Phi_k + c_k^{(\Phi\Phi)}\Phi_k^2\big] \right\rangle .$$

For uncorrelated ξ_k and Φ_k, we can write

$$F = 1 - M\big(F^{(\xi\xi)}\xi^2 + F^{(\xi\Phi)}\xi\Phi + F^{(\Phi\Phi)}\Phi^2\big) , \tag{112}$$
$$F^{(ij)} = \langle c^{(ij)}\rangle .$$

Formula (112) testifies to the accumulation of control errors: the errors in computation grow in proportion to the number M of elementary computational operations.

We adopt some numerical value F as a requirement for the quality of quantum computation to obtain the relation

$$\langle \xi^2 \rangle = \frac{1}{M}(1 - F)$$

between the admissible control errors $\langle \xi^2 \rangle$ and the number of possible computational operations M. For instance, if we assume that $F = 0.99$ and $\langle \xi^2 \rangle^{1/2} = 10^{-2}$, then the number of operations is $M = 10^2$. When the control inaccuracy is lowered to $\langle \xi^2 \rangle^{1/2} = 10^{-4}$ (0.01%), the number of operations is $M = 10^6$.

Therefore, the high level of control accuracy is the necessary condition for the realization of quantum computers. In impulse technology, oscillator frequencies are controlled with a high degree of accuracy; the control accuracy of the amplitudes of control fields needs to be improved in the future.

7.8 Decohering of qubits in multilevel systems

Two states of a multilevel system with 'suitable' properties are often selected as a qubit. For instance, when working with ions in a trap, it is possible to adopt the ground and excited optical energy levels of an ion as the qubit levels [5, 44]. The existence of other levels furnishes additional possibilities; they can be used as auxiliary levels in the performance of logical operations and the measurement of the qubit state.

At the same time, 'nonqubit' energy levels may form an additional decoherence channel arising from the 'leakage' of quantum information (population) from the qubit levels in the performance of logical operations. The transitions from the qubit levels to the nonqubit ones are effected as nonresonance transitions, whose probability rises with an increase in intensity of qubit-controlling resonance fields. The nonqubit energy levels fulfill the function of an additional 'environment' responsible for decohering the qubit. Possible ways of suppressing the decoherence of this type were proposed in Ref. [45].

7.9 Decohering in quantum operations

Control signals alter the qubit states during computations. Because the decohering $\mathrm{E}|\psi\rangle$ depends on the system state $|\psi\rangle$, it turns out that the computation process itself affects the decohering. That is why there is a need to consider the problem of decohering in the course of quantum operations. By way of example, we consider how decohering proceeds in the performance of the two-qubit CNOT operation [40, 47].

We represent the Hamiltonian of the system of qubits a and b as

$$H(t) = \sum \big[(\omega_n + \delta\omega_n)\sigma_z^{(n)} + (J_n + \delta J_n)\sigma_x^{(n)}\big] \\ + (g + \delta g)(\sigma_+^{(a)}\sigma_-^{(b)} + \sigma_-^{(a)}\sigma_+^{(b)}) , \qquad n = a, b . \tag{113}$$

The fluctuating parts of the Hamiltonian $\delta\omega_n\sigma_z^{(n)}$ and $\delta J_n\sigma_x^{(n)}$ may describe the phase and amplitude decoherence arising from both the interaction with the environment and the inaccuracy of control signals ω_n and J_n. The third term in

the sum accounts for the qubit interaction capable of giving rise to flip-flop type transitions.

To simplify the calculations as much as possible, we assume that the mean values of fluctuations are equal to zero and are δ-correlated:

$$\begin{aligned}
&\langle \delta\omega_n(t)\rangle = \langle \delta J_n(t)\rangle = \langle \delta g(t)\rangle = 0\,,\\
&\langle \delta\omega_n(t)\,\delta\omega_m(t')\rangle = \gamma_0\delta_{mn}\delta(t-t')\,,\\
&\langle \delta J_n(t)\,\delta J_m(t')\rangle = \gamma_1\delta_{nm}\delta(t-t')\,,\\
&\langle \delta g(t)\,\delta g(t')\rangle = \gamma_2\delta(t-t')\,.
\end{aligned}$$

The values of the parameters γ_0, γ_1, and γ_2 for a specific system are determined from measurements or calculated with the aid of microscopic interaction models.

Although the CNOT operation is an elementary quantum operation that belongs to the universal set of operations, it is executed with the aid of a sequence of rotations $\mathrm{U}_z(\alpha)$, $\mathrm{U}_x(\alpha)$ of the state vector of one qubit about the z and x axes by an angle α and the two-qubit flip-flop type operation $\mathrm{U}_j(\alpha)$ by an angle α [40]:

$$\begin{aligned}
\mathrm{U}_{\mathrm{CNOT}} = {}& \mathrm{U}_x^{(b)}\left(\frac{\pi}{2}\right)\mathrm{U}_z^{(b)}\left(-\frac{\pi}{2}\right)\mathrm{U}_x^{(b)}(-\pi)\,\mathrm{U}_j\left(-\frac{\pi}{2}\right)\\
&\times \mathrm{U}_x^{(a)}\left(-\frac{\pi}{2}\right)\mathrm{U}_j\left(\frac{\pi}{2}\right)\mathrm{U}_z^{(b)}\left(-\frac{\pi}{2}\right)\mathrm{U}_z^{(a)}\left(-\frac{\pi}{2}\right). \qquad (114)
\end{aligned}$$

The following notation was introduced in formula (114):

$$\begin{aligned}
&\mathrm{U}_z^{(n)}(\alpha) = \exp\left(\mathrm{i}\,\frac{\alpha}{2}\,\sigma_z^{(n)}\right),\\
&\mathrm{U}_x^{(n)}(\alpha) = \exp\left(\mathrm{i}\,\frac{\alpha}{2}\,\sigma_x^{(n)}\right),\\
&\mathrm{U}_j(\alpha) = \exp\left(\mathrm{i}\alpha(\sigma_+^{(a)}\sigma_-^{(b)} + \sigma_-^{(a)}\sigma_+^{(b)})\right).
\end{aligned}$$

The operation $\mathrm{U}_z^{(n)}(\alpha)$ is performed by turning on $\omega_n = -\varepsilon_0 \operatorname{sign}\alpha$ for a time $\tau = \alpha/2\varepsilon_0$, the operation $\mathrm{U}_x^{(n)}(\alpha)$ by turning on $J_n = -J_0 \operatorname{sign}\alpha$ for a time $\tau = \alpha/2J_0$, and the operation $\mathrm{U}_j(\alpha)$ by turning on $g = -g_0 \operatorname{sign}\alpha$ for a time $\tau = \alpha/g_0$. Here, $\operatorname{sign}\alpha = 1$ for $\alpha > 0$ and $\operatorname{sign}\alpha = -1$ for $\alpha < 0$. The total time of the CNOT operation performance is

$$\tau_{\mathrm{CNOT}} = \frac{\pi}{2\varepsilon_0} + \frac{\pi}{J_0} + \frac{\pi}{g_0}\,.$$

The fidelity parameter of the CNOT operation performance is defined as

$$F\big(|\psi(0)\rangle\big) = \langle\psi(t)|\rho_{\mathrm{CNOT}}|\psi(t)\rangle\,, \qquad (115)$$

where

$$\begin{aligned}
&|\psi(t)\rangle = \mathrm{U}_{\mathrm{CNOT}}^{(\mathrm{id})}|\psi(0)\rangle\,,\\
&\rho_{\mathrm{CNOT}}(t) = \mathrm{U}_{\mathrm{CNOT}}|\psi(0)\rangle\langle\psi(0)|\mathrm{U}_{\mathrm{CNOT}}^*\,,
\end{aligned}$$

with $\mathrm{U}_{\mathrm{CNOT}}$ being the matrices that contain inaccuracies arising from the fluctuations in Hamiltonian (113).

The parameter $F\big(|\psi(0)\rangle\big)$ is a function of the initial state of the system $|\psi(0)\rangle$. A more representative result is obtained by averaging $F\big(|\psi(0)\rangle\big)$ over some set of initial states $|\psi_{ij}(0)\rangle$:

$$F = \sum_{i,j=1}^{4}\frac{1}{4}\,F\big(|\psi_{ij}(0)\rangle\big)\,.$$

The following set of initial states for the first qubit was selected in Ref. [40]:

$$\begin{aligned}
&|\psi_1(0)\rangle = |0\rangle\,, \qquad |\psi_2(0)\rangle = |1\rangle\,,\\
&|\psi_3(0)\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\,, \qquad |\psi_4(0)\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + \mathrm{i}|1\rangle\big)
\end{aligned}$$

(and similarly for $j = 1, \ldots, 4$ for the second qubit).

Computer simulation was employed to obtain the plots of the dependence of the error $E(\gamma) = 1 - F(\gamma)$ on the root-mean-square fluctuation γ in the performance of the quantum CNOT operation. For $\omega_0 = J_0 = g_0 = 1$, the linear dependence $E \propto \gamma$ extends to values $\gamma \simeq 0.05$ (the weak noise mode). The effect is observed to be additive in the weak noise mode [40]:

$$E(\gamma_0, \gamma_1, \gamma_2) = E(\gamma_0, 0, 0) + E(0, \gamma_1, 0) + E(0, 0, \gamma_2)\,. \qquad (116)$$

The error $E(\gamma)$ attains the value 0.75 in the strong noise mode, when the state of the system becomes mixed.

7.10 Dependence of the decohering rate on the number of qubits in a computer

In Section 7.9, we calculated the rate of decohering γ_1 of the state of a single qubit. A full-scale quantum computer consists of more than a thousand qubits. Does the decoherence rate γ_n of computer states depend on the number of qubits n in it? The answer is affirmative. When the environments of different qubits are uncorrelated (incoherent), $\max\gamma_n = n\gamma_1$. When all qubits are embedded in the same (coherent) environment, $\max\gamma_n = n^2\gamma_1$.

A rigorous proof of these statements was obtained in Ref. [48] for the model of a qubit surrounded by oscillators. Here, we give a proof based on the notions developed above for a single qubit.

The initial nonentangled state of the computer and its environment is

$$|\psi(0)\rangle = \left(\sum_{x=0}^{2^n-1} c_x|x\rangle\right)|E(0)\rangle\,. \qquad (117)$$

Owing to the interaction between the computer and the environment, their states become entangled:

$$|\psi(t)\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle|E_x(x)\rangle\,. \qquad (118)$$

The nondiagonal entries of the reduced density matrix $\mathrm{Tr}_E\left(|\psi(t)\rangle\langle\psi(t)|\right)$ are given by

$$\rho_{x,x'}(t) = c_x c_{x'}^*\langle E_x(t)|E_{x'}(t)\rangle\,. \qquad (119)$$

The decohering consists in the decay (disappearance) of the nondiagonal entries of the density matrix $\rho_{x,x'}(t)$ (coherences $c_x c_{x'}^*$) as a result of the orthogonalization of the states of environment $E_x(t)$ and $E_{x'}(t)$ corresponding to different basis computer states $|x\rangle$ and $|x'\rangle$. When the environments of different qubits in the computer are uncorrelated,

$$\begin{aligned}
\langle E_x(t)|E_{x'}(t)\rangle &= \langle e_1^x e_2^x \ldots e_n^x|e_1^{x'} e_2^{x'} \ldots e_n^{x'}\rangle\\
&= \langle e_1^x|e_1^{x'}\rangle\langle e_2^x|e_2^{x'}\rangle \ldots \langle e_n^x|e_n^{x'}\rangle\\
&= \langle e_0|e_1\rangle^d\langle e_s|e_s\rangle^{n-d} = \langle e_0|e_1\rangle^d\,. \qquad (120)
\end{aligned}$$

In formula (120), we assumed that the states of d qubits in $|x\rangle = |i_1 \ldots i_n\rangle$ and $|x'\rangle = |j_1 \ldots j_n\rangle$ are different ($i_s \neq j_s$) and for $n-d$ qubits they coincide: $i_s = j_s$ (d is the Hemming distance between the basis computer states $|x\rangle$ and $|x'\rangle$). For a single qubit, $\langle e_0|e_1\rangle = \exp(-\gamma_1 t)$, and therefore

$$\langle E_x(t)|E_{x'}(t)\rangle = \exp(-d\gamma_1 t)\,.$$

Because $\max d = n$, it follows that $\max \gamma_n = n\gamma_1$.

In a more general form, the results in Ref. [48] for systems with incoherent and coherent environments are given by

$$\rho_{x,x'}(t) = \rho_{x,x'}(0)\exp\left(-\sum_{s=1}^{n}|i_s - j_s|\gamma_1 t\right), \qquad (121)$$

$$\rho_{x,x'}(t) = \rho_{x,x'}(0)\exp\left(-\left|\sum_{s=1}^{n}(i_s - j_s)\right|^2 \gamma_1 t\right). \qquad (122)$$

For a system with a coherent environment, the states of the 'Schrödinger cat' type $|0\ldots 0_n\rangle \pm |1\ldots 1_n\rangle$ experience the fastest possible decohering:

$$\gamma_n = \left|\sum_s (i_s - j_s)\right|^2 \gamma_1\,, \qquad \gamma_n = n^2\gamma_1\,.$$

At the same time, there are decoherence-free states. Such are the states wherein $i_s = 0$, $j_s = 1$ for one half of the qubits and $i_s = 1$, $j_s = 0$ (n is even) for the other half; then,

$$\sum_s (i_s - j_s) = 0\,, \qquad \gamma_n = 0\,.$$

An example of such a state is provided by the Bell states $|01\rangle \pm |10\rangle$ for two qubits.

The acceleration of decohering with the number of computer qubits, which was found to obey the law $\gamma_n = n\gamma$ (or $\gamma_n = n^2\gamma$), is supposedly the main obstacle in the path to the implementation of a full-scale quantum computer. When the performance of some calculation (algorithm) with a quantum computer requires a time t, the probability of obtaining the correct computational result decreases exponentially with n:

$$P = \exp(-\alpha n)\,, \qquad \alpha = \gamma t\,.$$

To arrive at the correct solution at least once, the computation should be repeated $k = \exp(\alpha n)$ times.

Under the conditions of rapid decohering, quantum algorithms cannot be executed efficiently, i.e., in a polynomial time. Executing Shor's n-digit number factorization algorithm requires the time $n^3\tau_{\rm op}$, which should be shorter than the decoherence time of the states of an n-qubit computer τ_1/n:

$$n^3\tau_{\rm op} < \frac{\tau_1}{n}\,,$$

where τ_1 is the decoherence time of a single qubit. Hence, there follows the condition for successful algorithm performance:

$$\frac{\tau_1}{\tau_{\rm op}} > n^4\,.$$

For $n = 10^3$, it is necessary to ensure the inequality $\tau_1/\tau_{\rm op} > 10^{12}$, which is many orders of magnitude greater than the value $\tau_1/\tau_{\rm op} \simeq 10^3 - 10^5$ in the practical cases under investigation. The aforesaid actually signifies that we should find a way of stabilizing the coherent state of a quantum computer for any desired time sufficient for the execution of a computation by a given algorithm of polynomial complexity. Among such methods are the quantum methods of error correction. Also proposed are different active techniques for the suppression of decoherence processes. These techniques are considered in the subsequent sections of the review.

To summarize this section, we emphasize the crucial role of decoherence in the emergence of classical properties of bodies. We classify bodies by the number of particles and the dimensions and time of decohering of the states of electron orbital motion calculated by the rule $\tau_n = \tau_1/n$:

Scale of the system	Number of particles	Volume, cm^3	Decoherence time, s
Atomic	1	10^{-23}	10^{-9}
Mesoscopic	10^3	10^{-20}	10^{-12}
Microscopic	10^{12}	10^{-12}	10^{-21}
Macroscopic	10^{23}	1	10^{-32}

The lifetime of coherent states of atomic and mesoscopic systems ($10^{-9} - 10^{-12}$ s) allows observing quantum coherent states with modern experimental techniques. The lifetimes of micro- and macroscopic bodies in quantum-coherent states ($10^{-21} - 10^{-32}$ s) are such that these states cannot be observed in present-day experiments. From the physical standpoint, there is no qualitative difference between atoms and macroscopic bodies, because both obey the laws of quantum mechanics. The difference is purely quantitative: to observe macroscopic bodies in quantum-coherent states requires experimental techniques with a temporal resolution of $10^{-20} - 10^{-30}$ s. These techniques are as yet unknown.

8. Methods for overcoming decohering effects in quantum computers

8.1 Information coding and error correction in a classical channel

Methods of coding and error correction in a quantum computer are the extension of methods developed for the purpose of error correction in the transmission of classical information via a classical channel. We demonstrate the essence of this method by the example of a classical binary symmetric channel whose properties are shown in Fig. 11. The schematic also describes the storage of information: in

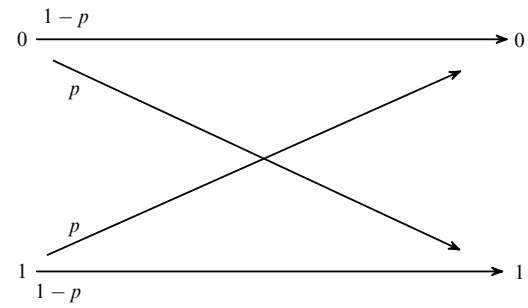

Figure 11. Schematic of a classical binary symmetric channel with an error probability p.

this case, the initial and final states are separated only by the storage time.

The classical three-bit majority code permits revealing and correcting one error in three bits, which occurred in the transmission via the channel. We assume that it is required to transmit the '0' bit value. We take two more reserve bits and encode '0' in three bits by forming the codeword '000'. In the transmission of the codeword with errors via the channel, each of the three bits may be inverted with a probability p. Let the third bit be inverted. This means that the bits arrive at the receiving end in the '001' state. We measure all three bits to discover the error in the third bit (by the majority principle). We correct the error by inverting the third bit. Decoding the corrected codeword '000', we obtain the correct state '0'. The error correction in the transmission of the bit in state '1' proceeds along similar lines.

We see that encoding one information bit in three physical bits (triplication) allows revealing and eliminating one error in three bits. Two (three) errors are not detected and not corrected by this code. For this code, the probability of error in the transmission of one information bit is $p_{\mathrm{er}} = 3p^2 + p^3$, $p_{\mathrm{er}} \ll p$ (errors in bits 1 and 2, 1 and 3, 2 and 3, or 1, 2, and 3). The ratio p/p_{er} is the factor by which the probability of error decreases when the above code is used.

8.2 Three-qubit quantum code

We apply the method of classical encoding of the state of one qubit into the state of three qubits:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \qquad |\psi_{\mathrm{c}}\rangle = \alpha|000\rangle + \beta|111\rangle\,.$$

This is easy to accomplish by applying the $\mathrm{CNOT}_{1,2}$ and $\mathrm{CNOT}_{1,3}$ operations. Let the codeword $|\psi_{\mathrm{c}}\rangle$ be transmitted with errors via the channel. We assume that the third qubit is inverted. As a result, the codeword $|\psi_{\mathrm{c}}^{(\mathrm{er})}\rangle = \alpha|001\rangle + \beta|110\rangle$ arrives at the receiving end of the channel. By measuring qubits in the basis $|0\rangle$, $|1\rangle$, we find '001' (with the probability $|\alpha|^2$) or '110' (with the probability $|\beta|^2$). Although we succeed in detecting the occurrence of error in the third bit, the α and β values are irretrievably lost in the measurement and the transmitted word $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is therefore lost.

The Quantum Error Correction (QEC) procedure in the form closest to the classical one comprises eight stages:

(1) An n-digit number $|x\rangle$ is specified, which should be transmitted via a channel with amplitude and phase errors. The number $|x\rangle$ may be a superposition of basis states, for instance, for one qubit, $|x\rangle = \alpha|0\rangle + \beta|1\rangle$.

(2) Encoding the n-digit quantum state $|x\rangle$ in the state of an $(n+k)$-digit register is fulfilled by the coding operator C:

$$\mathrm{C}|x\rangle|0\ldots0\rangle = \big|C(x)\big\rangle\,. \tag{123}$$

(3) The codeword $\big|C(x)\big\rangle$ is transmitted with errors along the channel characterized by the error operator $\mathrm{E} = \sum_i \mathrm{E}_i$, which acts on the codeword as

$$\Big(\sum_i \mathrm{E}_i\Big)\big|C(x)\big\rangle = \sum_i \big|\mathrm{E}_i\, C(x)\big\rangle\,. \tag{124}$$

(4) The error syndrome E_i is derived by the action of the error syndrome operator S:

$$\mathrm{S}\sum_i \big|\mathrm{E}_i\, C(x)\big\rangle|0\ldots0\rangle = \sum_i \big|\mathrm{E}_i\, C(x)\big\rangle|i\rangle\,. \tag{125}$$

Here, the indices i of the E_i error operators are written in an auxiliary register in the state $|0\ldots0\rangle$. The states $|i\rangle$ of the error syndrome register and the states $\big|\mathrm{E}_i\, C(x)\big\rangle$ of the register that stores the codeword with errors become entangled.

(5) In the computational basis, measurements are made of the states of the qubits of the register that stores the syndromes i of errors E_i:

$$\sum_i \big|\mathrm{E}_i\, C(x)\big\rangle|i\rangle \to \big|\mathrm{E}_s\, C(x)\big\rangle|s\rangle\,. \tag{126}$$

The measurement identifies the error that occurred in the channel (index error s, operator E_s).

(6) The error in the codeword derived from the measurements is corrected by the action of the inverse error operator E_s^{-1} on the register in the state $\big|\mathrm{E}_s\, C(x)\big\rangle$:

$$\mathrm{E}_s^{-1}\big|\mathrm{E}_s\, C(x)\big\rangle|s\rangle \to \big|C(x)\big\rangle|s\rangle\,. \tag{127}$$

The codeword is thereby made free of errors introduced by the channel.

(7) Decoding is performed:

$$\mathrm{C}^{-1}\big|C(x)\big\rangle|s\rangle \to |x\rangle|s\rangle\,.$$

(8) The auxiliary register $|s\rangle$ is returned to the initial state $|0\ldots0\rangle$ by the action on every register qubit with the operator that performs the transformation $|s_i\rangle \to |0_i\rangle$.

The above procedure appears to be somewhat abstract and obscure. A simple example with the transmission of a qubit in an arbitrary state along a channel with amplitude errors enables perceiving the significance of the procedures at all stages of the quantum error correction protocol.

(1) For a 'number' $|x\rangle$, we select the superposition $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ of the states of one qubit ($n = 1$).

(2) We encode the $|x\rangle$ state of one 'logical' qubit in the state $\big|C(x)\big\rangle$ of three ($n + k = 3$) 'physical' qubits. For this, we add two ancillary qubits in the $|00\rangle$ state to the qubit $|x\rangle$:

$$|x\rangle|00\rangle = \alpha|000\rangle + \beta|100\rangle\,.$$

Performing the unitary $\mathrm{CNOT}_{1,2}$ and $\mathrm{CNOT}_{1,3}$ transformations of the $|x\rangle|00\rangle$ state, which signify the encoding of the state $C|x\rangle$, we obtain the code state $|\psi_{\mathrm{c}}\rangle$ of the register of three physical qubits:

$$\begin{aligned}|\psi_{\mathrm{c}}\rangle \equiv \big|C(x)\big\rangle &= \mathrm{CNOT}_{1,3}\,\mathrm{CNOT}_{1,2}\big(\alpha|000\rangle + \beta|100\rangle\big)\\ &= \alpha|000\rangle + \beta|111\rangle\,.\end{aligned} \tag{128}$$

The procedure of encoding the 'number' $|x\rangle$ in the state $|\psi_{\mathrm{c}}\rangle$ of three qubits is completed.

(3) We write the error operator $\mathrm{E} = \sum_i \mathrm{E}_i$ that characterizes the channel in explicit form. We assume that the errors introduced by the channel consist in the flip of one of three qubits (amplitude decoherence). Then the error operator is

$$\begin{aligned}\mathrm{E} = \sum_{i=0}^{3} \mathrm{E}_i &= e_0(t)\,\sigma_0^{(1)}\sigma_0^{(2)}\sigma_0^{(3)} + e_1(t)\,\sigma_x^{(1)}\sigma_0^{(2)}\sigma_0^{(3)}\\ &\quad + e_2(t)\,\sigma_0^{(1)}\sigma_x^{(2)}\sigma_0^{(3)} + e_3(t)\,\sigma_0^{(1)}\sigma_0^{(2)}\sigma_x^{(3)}\,.\end{aligned} \tag{129}$$

Here, $\sigma_i^{(k)}$ are components of the Pauli operator that refer to qubit k, the operator $\sigma_x^{(k)}$ reverses the corresponding qubit, $\sigma_0^{(k)}$ is the identity matrix, and $\sum_{i=0}^{3} |e_i|^2 = 1$. We explicitly

write the code word with errors:

$$\mathrm{E}|\psi_{\mathrm{c}}\rangle = e_0(t)\,|\psi_{\mathrm{c}}\rangle + e_1(t)\big(\alpha|100\rangle + \beta|011\rangle\big)$$
$$+\, e_2(t)\big(\alpha|010\rangle + \beta|101\rangle\big) + e_3(t)\big(\alpha|001\rangle + \beta|110\rangle\big)\,. \quad (130)$$

If the time t is short in comparison with the decoherence time of the qubit state in the channel τ_{dc}, then $|e_1|$, $|e_2|$, $|e_3| \ll 1$, $|e_0| \simeq 1$. In superposition (130), all states $|x_1x_2x_3\rangle$, with the exception of $|\psi_{\mathrm{c}}\rangle$, contain one amplitude error.

(4) To the three qubits in the state $\mathrm{E}|\psi_{\mathrm{c}}\rangle$, we add three more auxiliary qubits in the state $|000\rangle$: $\mathrm{E}|\psi_{\mathrm{c}}\rangle \to \mathrm{E}|\psi_{\mathrm{c}}\rangle|000\rangle$. We define the error syndrome extraction operator S by the equality

$$\mathrm{S}|x_1x_2x_3000\rangle = |x_1x_2x_3\mathrm{CNOT}_{x_1,x_2}\mathrm{CNOT}_{x_1,x_3}\mathrm{CNOT}_{x_2,x_3}\rangle\,. \quad (131)$$

The S operator orders a pairwise comparison (by calculating CNOT) of the values of the variables x_1 and x_2, x_1 and x_3, and x_2 and x_3 in each of the three terms of the superposition $\mathrm{E}|\psi_{\mathrm{c}}\rangle$, and writing the result of calculations, $\mathrm{CNOT}_{x_i,x_j} = x_i \oplus x_j$ in the qubit states of the error syndrome register. For instance, if $|x_1x_2x_3\rangle = |100\rangle$, then $\mathrm{S}|100000\rangle = |100110\rangle$. This signifies that the amplitude error in the first qubit (1 in lieu of 0) has the syndrome $|110\rangle$ in the register that stores the syndrome. The syndromes of different errors calculated by rule (131) are collected in the table:

E_i	$\mathrm{E}_i\|000\rangle$	$\mathrm{SE}_i\|000000\rangle$	$\mathrm{E}_i\|111\rangle$	$\mathrm{SE}_i\|111000\rangle$
E_0	$\|000\rangle$	$\|000000\rangle$	$\|111\rangle$	$\|111000\rangle$
E_1	$\|100\rangle$	$\|100110\rangle$	$\|011\rangle$	$\|011110\rangle$
E_2	$\|010\rangle$	$\|010101\rangle$	$\|101\rangle$	$\|101101\rangle$
E_3	$\|001\rangle$	$\|001011\rangle$	$\|110\rangle$	$\|110011\rangle$

(5) We perform the state measurements of the three last-mentioned qubits, which carry information about the error syndrome, in the register of six qubits in the state $\mathrm{SE}|\psi_{\mathrm{c}}\rangle$. In their measurement, we obtain one of the four possible $y_1y_2y_3$ syndrome values: 000, 110, 101, 011, with the respective probabilities $|e_0|^2$, $|e_1|^2$, $|e_2|^2$, $|e_3|^2$. The measurement result determines which of the operators E_s produces the error.

(6) We correct the error revealed:

$$\mathrm{E}_s^{-1}\mathrm{E}_s|\psi_{\mathrm{c}}\rangle = |\psi_{\mathrm{c}}\rangle|y_1y_2y_3\rangle\,.$$

(7) We decode the codeword:

$$\mathrm{C}^{-1}|\psi_{\mathrm{c}}\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big)\,.$$

(8) The qubits in which the syndrome is written are returned to the state $|000\rangle$ by applying the σ_x operator to the qubits in the state $y_i = 1$.

In the course of error correction in a single qubit, we need not resort to additional qubits for writing the error syndrome. The protocol scheme is diagrammed in Fig. 12. The transformations of the initial state of three qubits prescribed by the scheme

$$\big|\psi(0)\big\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big)|0\rangle|0\rangle \quad (132)$$

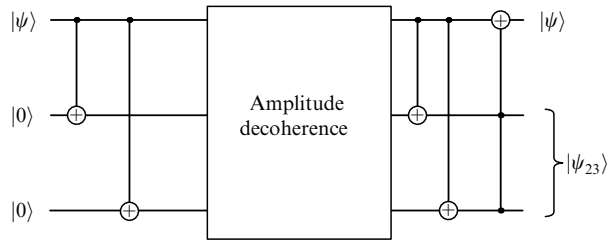

Figure 12. Schematic representation of the protocol for correcting a quantum amplitude error.

lead to the initial state

$$\big|\psi(t)\big\rangle = \big(\alpha|0\rangle + \beta|1\rangle\big)\big[e_0(t)|00\rangle + e_1(t)|11\rangle$$
$$+\, e_2(t)|10\rangle + e_3(t)|01\rangle\big]\,. \quad (133)$$

The decoding transformation $\mathrm{CNOT}_{23,1}$ has set the first qubit free from the amplitude error and from entanglement with the second and third qubits. The errors introduced by the E operator are 'collected' in the final entangled state of the second and third qubits: added to their initial $|00\rangle$ state are the $|11\rangle$, $|10\rangle$, and $|01\rangle$ states, which contain errors. Upon determining the state of these qubits by measurement, they should be returned to their initial state $|00\rangle$.

8.3 Correction of phase errors

In Section 8.2, we presented the correction protocols of amplitude errors in the qubit state introduced by operator (129). We now discuss the phase errors introduced by the operator

$$\mathrm{E} = e_0(t)\,\sigma_0^{(1)}\sigma_0^{(2)}\sigma_0^{(3)} + e_1(t)\;\sigma_z^{(1)}\sigma_0^{(2)}\sigma_0^{(3)}$$
$$+\, e_2(t)\;\sigma_0^{(1)}\sigma_z^{(2)}\sigma_0^{(3)} + e_3(t)\;\sigma_0^{(1)}\sigma_0^{(2)}\sigma_z^{(3)}\,. \quad (134)$$

The phase error operator differs from the amplitude error operator by the change $\sigma_x^{(k)} \to \sigma_z^{(k)}$. Phase errors are a purely quantum effect and are absent in classical computations.

The protocol for correcting phase errors in the qubit state in the three-qubit code is schematized in Fig. 13. Added to the previous scheme of encoding the state of the first qubit in the state of three qubits are the Hadamard transformations H of each qubit. The encoding results in the code state

$$|\psi_{\mathrm{c}}\rangle = \alpha|+++\rangle + \beta|---\rangle\,, \quad (135)$$

$$|+\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\,,$$
$$|-\rangle = \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)\,, \quad (136)$$

$$\mathrm{H}|-\rangle = |1\rangle\,, \qquad \mathrm{H}|+\rangle = |0\rangle\,. \quad (137)$$

The phase error operators $\sigma_z^{(k)}$ in the basis $|+\rangle$, $|-\rangle$ act as amplitude operators that revert the states $|+\rangle$, $|-\rangle$:

$$\sigma_z|+\rangle = |-\rangle\,, \qquad \sigma_z|-\rangle = |+\rangle\,.$$

Considering the properties of these transformations, it is easily shown that the scheme given in Fig. 13 transforms the initial state of the three qubits

$$\big(\alpha|0\rangle + \beta|1\rangle\big)|00\rangle$$

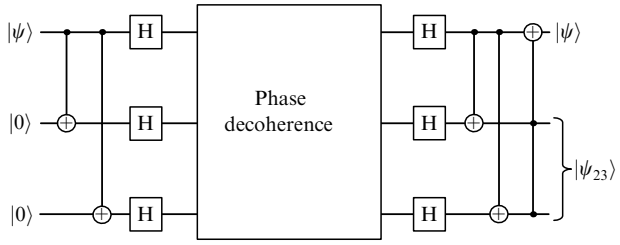

Figure 13. Schematic representation of the protocol for correcting a quantum phase error.

into the final state

$$\big(\alpha|0\rangle + \beta|1\rangle\big)\big(e_0|00\rangle + e_1|11\rangle + e_2|10\rangle + e_3|01\rangle\big)\,.$$

When both amplitude and phase errors emerge in a computer, such that $E = E_{\rm amp} + E_{\rm ph}$, the error correction protocol should furnish the protocol performance by the schemes given in Figs 12 and 13.

For simplicity, the construction principles of quantum error correction protocols were demonstrated by the example of the simplest three-qubit code. This code enables detecting and eliminating one error (an amplitude or phase error) in three qubits. Codes involving five and seven qubits have been elaborated, enabling the correction of any error (an amplitude or phase error) in one qubit [49, 50]. Shor's nine-qubit code makes it possible to correct two errors — a phase error and an amplitude error [15].

8.4 Fault-tolerant quantum computations

An analysis of the quantum error correction method demonstrates its universality with respect to any error sources. All errors are divided into amplitude and phase errors; errors of both kinds are corrected by quantum error correction methods.

When performing the protocols of quantum error correction, use is made of the same elementary operations as in quantum computations. A quantum computer should operate by alternating computations with error correction protocols.

The capabilities of the error correction method are determined by the code selected: the code allows correcting only those errors for which it was designed. For instance, the three-qubit code allows correcting one error in three qubits. Two errors in three qubits cannot be corrected by this code. The code should be adopted on the basis of the study of error sources (decoherence mechanisms) in a quantum computer.

The codes used in quantum error correction methods require additional resources: an increase in the number of qubits (redundancy) and the number of quantum operations. For a single-step encoding, the number of requisite qubits increases approximately ten-fold. When use is made of concatenated encoding, the number of qubits increases by about a factor of 10^t, where t is the number of encoding cascades [55]. The number of quantum operations used in the protocols of quantum error correction increases with the same rate. This brings up the question: is it possible to stabilize the quantum-coherent computer state for practically acceptable qubit and operation 'expenses' for error correction?

Error-correction operations themselves introduce additional errors owing to inaccuracies in the performance of quantum operations, as well as due to decohering effects in the quantum computer.

Quantum computation is termed fault-tolerant if it furnishes a reliable computational result under the aforementioned limitations of error correction methods. The computations are fault-tolerant if the error correction procedures remove more errors from the computer than they introduce. Emphasis is placed on the requirement that no multiplication of the errors introduced by correction procedures occurs. The periodicity of correction procedures should be such that the error accumulated between two QEC procedures is below the level of errors under correction.

The noise immunity of computations actually signifies the stabilization of the quantum coherent computer state for the time required to execute a polynomial algorithm. The conditions for noise-immune computations with a quantum computer are presently formulated as follows: the quantum computer can operate for an arbitrarily long time if the error probability ε in one elementary quantum operation is below the threshold value $\varepsilon_{\rm th}$. The numerical value of $\varepsilon_{\rm th}$ is estimated by numerical simulations of quantum computer operation; modern estimates yield a value $\varepsilon_{\rm th} \leqslant 10^{-5} - 10^{-4}$ [52].

8.5 Decoherence-free states of a quantum computer

Actively discussed in the literature is the possibility of employing the so-called decoherence-free states of a quantum computer in quantum calculations. We assume that the mechanism of qubit decohering that operates in the computer is known: let it be defined, for instance, by the operator

$$\mathrm{E} = |e_0\rangle\sigma_0^{(1)}\sigma_0^{(2)} + |e_1\rangle\sigma_x^{(1)}\sigma_x^{(2)}\,.$$

If the states of a logical qubit $|0\rangle_{\rm L}$ and $|1\rangle_{\rm L}$ are encoded into the symmetric states of two physical qubits,

$$|0\rangle_{\rm L} = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)\,, \qquad |1\rangle_{\rm L} = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)\,, \qquad (138)$$

these states are invariant under the action of the error operator E.

The limited nature of the above way of suppressing decoherence is evident. The code subspace of states is free from decoherence only relative to one mechanism; in real physical systems, there are several suchlike mechanisms. Lastly, always present is the mechanism related to the qubit control channel: control errors.

8.6 Decoherence-immune qubits

Bacon et al. [53] proposed designing qubits in such a way as to prohibit decohering for energy reasons (a 'supercoherent qubit'). We consider a system of spins $S = 1/2$ coupled pairwise by the exchange interaction

$$H^{(n)} = \frac{\varDelta}{2}\left[\sum_{i,j=1}^{n}\big(S^{(i)}S^{(j)}\big) + \frac{3}{4}\,nI\right]. \qquad (139)$$

Hamiltonian (139) can be represented as

$$H^{(n)} = \frac{\varDelta}{2}\,S^{(n)\,2}\,,$$

where $S^{(n)} = \sum_{i=1}^{n} S^{(i)}$ is the total spin of the system. The eigenvalues and eigenfunctions of $H^{(n)}$ for even n take the

form

$$E_{J_n} = \frac{\Delta}{2} J_n(J_n+1)\,, \qquad J_n = 0, \ldots, \frac{n}{2}\,, \tag{140}$$

$$|\psi_{J_n}\rangle = |\lambda, J_n, m\rangle \tag{141}$$

(λ is the degeneracy of the state).

The ground level $E_0 = 0$ of the system for $n = 4$ is doubly degenerate ($\lambda = 2$); the states of this doublet are suggested for the qubit states. Some additional interaction in the system is required to remove the degeneracy and make the qubit states distinguishable. The lowest excited level E_1 of the system has the energy $E_1 = \Delta$. The decoherence operator of the general form

$$\mathrm{E} = e_0\sigma_0 + e_x\sigma_x + e_y\sigma_y + e_z\sigma_z\,,$$

which acts on the spin of a single particle in the system $H^{(n)}$, gives rise to transitions from the ground level by the selection rule $\Delta J_n = 1$, i.e., the $E_0 \to E_1$ transitions. At low temperatures ($kT \ll \Delta$), the probability of these transitions is exponentially low:

$$w_{0\to 1} \propto \exp\left(-\frac{\Delta}{kT}\right).$$

Despite the attractiveness of the idea of a 'supercoherent qubit', it is evident that there exist other channels of qubit decohering apart from those mentioned above. Because an interaction is introduced into the system to split the doubly degenerate ground energy level of the system, the noise accompanying this interaction produces a new decoherence channel. To perform one- and two-qubit operations, we have to set up channels for controlling individual qubits and their interaction. This signifies the emergence of new decoherence channels due to fluctuations in control signals. In view of the aforesaid, we may draw the conclusion that a 'supercoherent qubit' may be free from only a part of decoherence channels; other channels persist.

8.7 Methods for preventing errors: the quantum Zeno effect

The so-called error prevention protocol was proposed in Refs [54, 55]. In essence, this is a slightly modified protocol of quantum error correction. Once again, we write the state of the system at the stage of error syndrome derivation:

$$\mathrm{S}\sum_i \left|\mathrm{E}_i\, C(x)\right\rangle |0\ldots 0\rangle = \sum_i \left|\mathrm{E}_i\, C(x)\right\rangle |i\rangle\,. \tag{142}$$

At this stage, the system states $\left|\mathrm{E}_i\, C(x)\right\rangle$ become entangled with the states $|i\rangle$ of the error syndrome register.

The error operator $\mathrm{E} = \sum_i \mathrm{E}_i$ is represented as the sum $\mathrm{E} = \sum_i e_i(t)\,\mathrm{E}_i$. Here, E_i are the error operators proper and $e_i(t)$ are the probability amplitudes, which depend on the time t during which the operator E acts on the system. The term $e_0(t)\,\mathrm{E}_0$ stands out in the sum, where E_0 is the identity operator and the amplitude

$$e_0(t), \quad e_0(0) = 1\,,$$

defines the probability that the system survives in the initial (error-free) state $C(x)$:

$$p_{\mathrm{suv}}(t) = \left|e_0(t)\right|^2, \qquad p_{\mathrm{suv}}(0) = \left|e_0(0)\right|^2 = 1\,.$$

On the contrary, the amplitudes

$$e_{i\neq 0}(t), \quad e_{i\neq 0}(0) = 0\,,$$

increase with the time t during which the operators $\mathrm{E}_{i\neq 0}$ act on the system.

In view of the aforesaid,

$$\left|\mathrm{SE}\, C(x)\right\rangle |0\ldots 0\rangle = \sum_i e_i(t) \left|\mathrm{E}_i\, C(x)\right\rangle |i\rangle\,. \tag{143}$$

In the measurement of the state of error syndrome register qubits $|i\rangle$, entangled state (143) reduces to one of the non-entangled states $\left|\mathrm{E}_s\, C(x)\right\rangle |s\rangle$. The probability of the corresponding result is $\left|e_s(t)\right|^2$. If the time t is so short that

$$\left|e_0(t)\right|^2 \leqslant 1\,, \quad \left|e_i(t)\right|^2 \ll 1\,, \quad i \neq 0\,,$$

the measurement of the register state $|i\rangle$ yields the initial error-free state $\mathrm{E}_0\left|C(x)\right\rangle = \left|C(x)\right\rangle$ with a probability close to unity. This concludes the error prevention protocol. (It only remains to bring back the register $|i\rangle$ to the initial state $|0\ldots 0\rangle$.) Because the error correction stage is absent in the protocol, the $|i\rangle$ register size may be reduced to a minimum; a saving of the requisite qubit number occurs [55].

The error prevention protocol corresponds closely to the quantum Zeno effect, which is the subject of numerous publications [54–59]. The quantum Zeno effect belongs to the so-called active methods of decoherence suppression: the experimenter performs direct measurement of the state of the system status to suppress decoherence.

By solving the Schrödinger equation (see Section 7.5), we obtained two different expressions for the probability of survival of the initial state $\left|e_0(t)\right|$:

$$\left|e_0(t)\right|^2 = 1 - at^2\,, \quad t \ll \frac{2\pi}{\omega_l - \omega_0}\,, \quad \hbar\left(\sum_l |\lambda_l|^2\right)^{-2}, \tag{144}$$

$$\left|e_0(t)\right|^2 = \exp(-\gamma t) \simeq 1 - \gamma t\,, \quad t \gg \frac{2\pi}{\omega_l - \omega_0}\,, \quad \hbar\left(\sum_l |\lambda_l|^2\right)^{-2}, \tag{145}$$

where

$$a = \hbar^{-2}\left(\sum_l |\lambda_l|\right)^2.$$

The quadratic dependence $p_{\mathrm{suv}}(t) = 1 - at^2$, which is characteristic of very short times t, is the necessary condition for the observation of the quantum Zeno effect: the periodic measurement of the system signal state at intervals t that satisfy the inequality in (144) preserves the system in the initial state.

Indeed, we select an arbitrarily long time T and perform T/t measurements of the system at intervals t. Then, the probability of survival of the initial system state is

$$p_{\mathrm{suv}}(T) = (1 - at^2)^{T/t} = 1 - aTt\,, \quad \lim_{t\to 0} p_{\mathrm{suv}}(T) = 1\,. \tag{146}$$

On the contrary, if measurements are made at intervals t such that the system evolution obeys the conditions in (145), the Zeno effect is absent:

$$p_{\mathrm{suv}}(T) = (1 - \gamma t)^{T/t} \simeq 1 - \gamma T \to 0\,, \qquad T \to \frac{1}{\gamma}\,. \tag{147}$$

The limitations on the possibility of realizing the Zeno effect in quantum computers are evident. The duration of measurements τ repeated at time intervals t should satisfy the condition $\tau \ll t$. The parameters of short pulses are very hard to control; the fluctuations of pulse parameters open up a new decoherence channel. Many combinations of the parameters give rise to precisely the acceleration of decohering (the anti-Zeno effect) [59]. The feasibility of performing computational unitary operations against the background of periodic system status measurements is not evident. If the Zeno effect were actually realized, it would be beneficial as a method of information storage in the quantum computer memory.

8.8 Dynamic methods of decoherence suppression

Viola and Lloyd [60] proposed a dynamic method of decoherence suppression close in performance technology to the method of the quantum Zeno effect. Frequent measurements of the system status inherent in the Zeno method are replaced in this case with frequent control pulses whose power (area) is selected such that every pulse inverts the state of a qubit (spin, quasi-spin). This approach is efficient where phase qubit decoherence is involved, when the energy of interaction with the environment is

$$H_{\text{int}} = \hbar\sigma_z B\,,$$

where σ_z is the qubit quasi-spin and B are environmental variables. Under inversions of the qubit quasi-spin σ_z, the interaction energy H_{int} changes sign, and hence the time-average value $\langle H_{\text{int}}\rangle = 0$, i.e., multiple spin inversion isolates the qubit from the environment.

Another interpretation of this effect is possible: changing the energy interaction sign is equivalent to changing the sign of time in the evolution operator $U(t) = \exp(-\mathrm{i}H_{\text{int}}t)$; during the two time intervals that follow two spin-inverting pulses, the evolution proceeds in opposite directions to cancel each other. The proposed method is a direct development of the spin echo and refocusing techniques elaborated in NMR spectroscopy.

Theory allows determining the method applicability criteria: the qubit is asymptotically decoupled from the environment if the number of pulses $N = T/\Delta t \to \infty$, where Δt is the time interval between the pulses. In the limit of fast spin flips, the spin decohering is suppressed for any temperature and surrounding oscillator spectrum if $\Delta t \leqslant \tau_{\text{c}}$, where τ_{c} is the correlation time of environmental variables. Broadly speaking, the condition $\Delta t \leqslant \tau_{\text{c}}$ is hard to realize in practical cases. An advantage of the method is the fact that no additional qubits are required.

8.9 Quantum error correction by the method of weak continuous measurements and feedback

Milburn and his collaborators investigated the protocol of quantum error correction reliant on weak continuous measurements and control of qubit states by feedback signals [61, 62]. In classical systems, control circuits with feedback exhibit a high efficiency; that is why there is good reason to investigate suchlike schemes for quantum systems as well.

As in the protocols with discrete strong measurements described above, the state of n qubits is encoded into the state of $m > n$ qubits in the code subspace C. The Pauli operators σ_x, σ_y, and σ_z are employed to form the stabilizing generators $g = \prod \sigma_i^{(a)}\sigma_j^{(b)}\ldots$ such that $g|\psi_{\text{c}}\rangle = |\psi_{\text{c}}\rangle$. Discrete strong measurements g are used for error syndrome determination.

A similar protocol of error correction with the aid of weak continuous stabilizing generator measurements and feedback comprises the following procedures:

(1) encoding the $|\psi\rangle$ state of n qubits into the $|\psi_{\text{c}}\rangle$ state of $m > n$ qubits;

(2) continuous weak g measurements;

(3) filtration of measurement currents with the aid of a low-frequency filter to reduce noise in the measurement signal;

(4) '+' or '−' sign determination of the smoothed current signal and formation of the feedback signal for every qubit with the inclusion of the information about the signal signs;

(5) application of the feedback signal to every qubit.

Mathematical simulations performed for a three-qubit code ($n = 1$, $m = 3$) suggest that the protocol involved is efficient for low noise levels ($\gamma \leqslant 0.1$). The method is inefficient for high noise levels ($\gamma > 0.3$). Moreover, in the conditions of strong noise, the protocol leads to a faster decrease in the fidelity parameter $F(t)$ than in the absence of the procedure. For a high procedure repetition frequency, discrete methods of error correction are more efficient than the methods with continuous weak measurements and feedback: $\Delta t \ll \gamma^{-1}$. For $\Delta t > \gamma^{-1}$, the method with discrete measurements is also inefficient.

The protocols with discrete measurements may turn out to be useful in preserving the qubit states in the memory systems of quantum computers. Whether continuous measurements can be combined with computational unitary transformations remains to be seen.

8.10 Fault-tolerant topological quantum computations

By invoking the geometrical properties of the state space of quantum systems, it is possible to construct a universal set of quantum operations immune to control errors [64]. These properties are clearly manifested in the description of qubit states by the density matrix

$$\rho(s) = \frac{1}{4}\left(I + \sum_i s_i\sigma_i\right), \qquad i = x, y, z\,. \tag{148}$$

Pure qubit states are defined with a unit Bloch vector **s** with real components s_x, s_y, s_z.

The rules for going over from the parameters s_x, s_y, s_z to the parameters $|a|$, $|b|$, $|\varphi|$ of the state vector

$$|\psi\rangle = \begin{vmatrix} |a| \\ |b|\exp(\mathrm{i}\varphi) \end{vmatrix}$$

are determined from the equality

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{4}\left(I + \sum s_i\sigma_i\right)$$

and are given by

$$\begin{aligned} 1 + s_z &= 2|a|^2\,, \qquad s_x + \mathrm{i}s_y = 2ab^*\,, \\ 1 - s_z &= 2|b|^2\,, \qquad s_x - \mathrm{i}s_y = 2a^*b\,. \end{aligned} \tag{149}$$

In the state

$$|0\rangle = \begin{vmatrix} 1 \\ 0 \end{vmatrix},$$

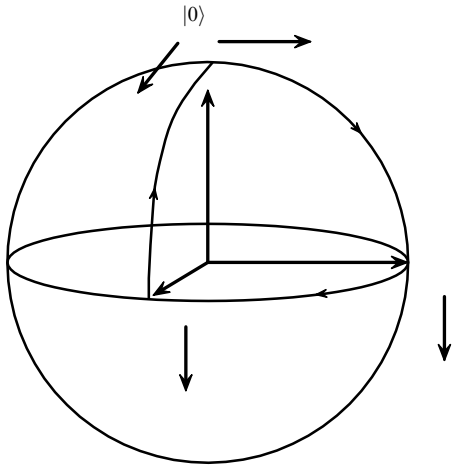

Figure 14. Schematic of the emergence of geometric phase difference in the quantum qubit state caused by the curvature of qubit state space.

which corresponds to the Bloch vector $\mathbf{s}(0,0,1)$, the phase remains indefinite; it can be given any value $0 \leqslant \varphi < 2\pi$. The surface of the unit sphere $s_x^2 + s_y^2 + s_z^2 = 1$ is the curved (nonplanar) space of pure qubit states. The space curvature is $k = r^{-2} = 1$.

The curvature of the state space gives rise to the so-called geometric phase by cyclic (closed) trajectories in the state space. We select, for instance, the trajectory from the North Pole of the Bloch sphere down to the equator along the meridian in the Oyz plane, along the equator to the Oxz plane, and up the meridian to the North Pole (Fig. 14):

$$\mathbf{s}(0,0,1) \to \mathbf{s}(0,1,0) \to \mathbf{s}(1,0,0) \to \mathbf{s}(0,0,1)\,.$$

We select the phase vector of the initial state as a unit vector in the plane of the drawing along the tangent (at the point of the North Pole). In the course of the cyclic process, there occurs a parallel transfer of the phase vector: the vector retains the tangent direction at each point of the trajectory. On returning to the initial point, we find that the qubit phase vector makes the angle $\gamma = \pi/2$ relative to the initial orientation direction. The source of the resultant phase difference is the geometric property of the state space: its curvature; hence the name of the resultant phase, the geometric phase.

In general, $\gamma = k\Omega$, where Ω is the solid angle subtended by the closed trajectory and k is the curvature of the surface of states. In our case, $k = 1$, $\Omega = \pi/2$, and $\gamma = \pi/2$. The phase γ is conveniently represented as

$$\begin{vmatrix} a \\ b \end{vmatrix} \to \begin{vmatrix} a \exp\left(-\mathrm{i}\,\dfrac{\gamma}{2}\right) \\ b \exp\left(\mathrm{i}\,\dfrac{\gamma}{2}\right) \end{vmatrix}.$$

In an adiabatic process first considered by Berry [65], the phase is

$$\gamma = \int_s \left\langle \psi(s) \left| \frac{\mathrm{d}}{\mathrm{d}s} \right| \psi(s) \right\rangle \mathrm{d}s\,, \tag{150}$$

where s is the system parameter employed to control the adiabatic cyclic process. The value of geometric phase can be calculated by the Pancharattam formula

$$\gamma = \arg\left\{\langle\varphi_1|\varphi_2\rangle\langle\varphi_2|\varphi_3\rangle \ldots \langle\varphi_4|\varphi_1\rangle\right\},$$

when the cycle is defined by the states at discrete points [64].

The relation $\gamma = k\Omega$ signifies that the geometric phase is basically dependent on the shape of the system trajectory in the state space. The noise immunity of phase gates (operations) employing the geometric phase consists in the fact that the trajectory form fluctuations (due to control errors) are averaged to become zero with retention of the value of the solid angle Ω [64].

The idea of a stronger ('topological') immunity of the phase gate to control errors is easy to explain by the example of a phase gate employing the Aharonov–Bohm phase difference. When the electron wave function flows over a magnetic flux Φ enclosed in a thin solenoid, the phase difference between the two parts of the wave function is $\gamma = e\Phi/\hbar c$ and is independent of the form of the ambient electron wave function components. This topological property makes the phase gate immune to control errors.

Commutative $\left(\exp(\mathrm{i}\gamma_1)\exp(\mathrm{i}\gamma_2) = \exp(\mathrm{i}\gamma_2)\exp(\mathrm{i}\gamma_1)\right)$ geometric phases are referred to as Abelian. To construct universal topological calculations immune to control errors, it is necessary to have operations of the non-Abelian type (noncommutative). Ways of constructing non-Abelian phase operations harnessing the fractional Hall effect (anyons) have been proposed [66]. The possibility of constructing phase operations with the geometric phase involving ions in traps has also been considered [67].

8.11 On the possibility of combined use of different methods of error correction

An important issue in the theory of methods of error correction in quantum computers is the possibility of combined use of these methods in real situations, because there is no certainty that any one of them taken alone would afford long-term stabilization of computations. It is also unclear whether it will be possible to employ one decoherence suppression procedure or another simultaneously with computations. From the standpoint of computation acceleration, it is desirable that the decoherence suppression procedures should be performed simultaneously with computations. Evidently, this is not always possible.

In the preceding sections, we convinced ourselves that quantum error correction procedures use the same elementary computational operations and the same qubit-control devices as quantum computation itself. Under these conditions, the procedures of quantum error correction and computation are performed during different time intervals but alternately. Byrd and Lidar [68] investigated the conditions for the simultaneous application of the methods of quantum error correction and the dynamic methods involving short pulses that isolate qubits from the environment. Determining the conditions for the application of other combinations of error correction techniques and decoherence suppression is a topical problem.

9. The search for ways to implement quantum computers: experimental research

In the framework of this review, there is no way of outlining the experimental results concerning the quest for approaches to the realization of the idea of quantum computers. We

mention monographs [14, 30] as experimental works and reviews covering separate areas of the quest [5, 25, 44]. Here, we restrict ourselves to the enumeration of the avenues of the quest and brief comments.

The method of nuclear magnetic resonance in liquids at room temperature made it possible to demonstrate the experimental performance of principal quantum algorithms and error correction techniques involving up to seven qubits in an ensemble quantum computer [25]. However, upon establishing the fact that the qubits in an NMR quantum computer in room-temperature liquids are limited to about ten in number, the effort mounted to advance this line was presumably weakened.

A large number of experiments in the realization of quantum computational operations were performed on ions in a one-dimensional ionic crystal in the Paul trap [5, 44]. This version of a quantum computer, too, encountered serious obstacles to increasing the number of qubits (ions in the one-dimensional crystal) owing to the instability of the one-dimensional crystal. The found limitations of the number of qubits may be overcome by resorting to an ensemble of many traps. In this case, it is necessary to develop methods for fast (in a time comparable with the time of quantum operations) ion transportation from one trap to another. The ion transportation was shown to be basically possible [69].

A qubit arrangement similar to ionic crystals can be realized in semiconductor crystals of a spinless single-isotope ^{28}Si silicon crystal, in which ^{31}P phosphorus atoms (qubits) are arranged in a linear chain (Kane's model [7]). The function of a qubit is fulfilled by the nuclear $(I = 1/2)$ or electron $(S = 1/2)$ spin of atomic phosphorus ^{31}P. The number of qubits 'prepared' in this architecture is unlimited. The pace of development of this direction, which is generally believed to be highly promising, is determined by the rate of nanotechnology developments required to fabricate the structures with the requisite parameters. A difficult problem in this quantum computer realization is the state measurement of a single spin qubit. The qubit state measurement problem is mitigated if recourse is made, as we proposed, to the ensemble version of the qubit [30].

Experimental research is vigorously pursued to make qubits reliant on the electrons in semiconductor quantum dots [70, 71]. The orbital or spin states of a single electron in the quantum dot are being investigated for the qubit states. In this method, the number of qubits (quantum dots with a single electron) is not limited, either.

Qubits based on superconducting mesostructures have been prepared and investigated [71]. In this case, two qubit versions have been made: in the first version, quantum information is encoded into the number of superconducting pairs in a quantum dot, and in the second version, into the direction of the superconducting current in a SQUID. To fabricate qubit structures, use is made of the available microelectronic technologies. The number of qubits packed on a 'chip' is basically unlimited. This line of investigation into ways of realizing quantum computers is characterized by an intense activity of experimenters and steady progress.

A large number of experiments in the realization of quantum operations have been performed with solitary atoms in microcavities (cavity quantum electrodynamics). The model of a quantum system is a two-level atom-qubit coupled to an oscillator-photon in one of the cavity oscillation modes. The experimental works are outlined in monograph Ref. [14]. Unfortunately, it is not clear how to increase the number of qubits in this method. Conceivably, this method could prove to be useful in the development of atomic and photon qubit transport, as well as in the quantum information transfer from atomic qubits to photon ones and vice versa (an atom – photon quantum interface).

Of interest is the possibility of realizing quantum operations using linear optical elements (an 'optical quantum computer') [72]. In this method, the number of optical elements grows exponentially with the number of qubits in the computer. The experiments along this line of quantum computer realization actually merge with experiments in the area of quantum optics [73].

The above-enumerated lines of research into ways to realize a quantum computer rely on technologies elaborated for other purposes (time-standard development, microelectronic, and quantum-optical technologies). Other promising ideas that may call for the development of radically new technologies have also been conceived. We list some of them:

(1) a two-dimensional electronic crystal in a potential well near the surface of liquid helium [74] (the physics of these crystals has been well studied; the function of qubits may be fulfilled by the spins of individual electrons in the crystal);

(2) a two-dimensional atomic lattice in an optical trap formed by the standing wave of interfering laser beams [75];

(3) anyons in a two-dimensional electron gas in semiconductors under the conditions of the fractional Hall effect [66];

(4) quantum cellular automata in ferromagnetic (antiferromagnetic) structures in crystals [76].

Recent progress in experiments with Bose – Einstein condensates opens up the possibility of searching for quantum operations employing these new quantum systems [77].

10. Conclusion

10.1 Quantum computers: a dream or reality?

The research in the area of quantum computers and quantum computation is currently at the stage of development of basic problems. This stage should be concluded with the selection of one of the approaches of quantum computer realization as the main one. Most likely, several prototypes of a quantum computer relying on different technologies will have to be made and compared to chose one for subsequent development.

As of now, there exists a wide diversity of opinions regarding the future of quantum computers — from predictions of the (unavoidable) forthcoming quantum technical revolution to a deep scepticism. In a concentrated form, the 'pro' and 'con' opinions were expressed, for instance, in the dispute of participants at the conference on quantum computation (June 2003) [46]. We list the 'con' arguments:

(1) Quantum computers are unnecessary: there are no problems that justify the development and implementation of a quantum computer. Only two efficient quantum algorithms (Shor's and Grover's) have been found over the past years. It is meaningless to make a quantum computer solely for the purpose of cracking the popular modern RSA cryptosystem: it will have become a thing of the past by the time the quantum computer makes its appearance.

(2) A quantum computer is a special-purpose analog device, which is hard to realize.

(3) Nature did not opt to select the quantum method of calculations: the brain does not perform quantum operations.

We do not reproduce the 'pro' arguments, for we believe that our entire review is argumentation in support of quantum computers.

10.2 What next?

Let us assume that an age will dawn when the quantum dynamics of systems will be mastered at the atomic level and quantum information-processing technology will be developed. What next? What new resources of nature might be harnessed to create new-generation information technologies? The degrees of freedom in systems of a smaller volume than the atom (atomic nuclei, elementary particles) are associated with high energies, which hinders their use for information encoding. Does this signify that all informational resources of nature will be exhausted at the atomic level?

10.3 On the content and structure of the modern course in quantum mechanics

When we compare ordinary textbooks of classical and quantum mechanics, it is easy to see their differences in content and structure. A course in classical mechanics is subdivided into statics and dynamics, while this division is absent in a course on quantum mechanics. It is dominated by statics (system eigenvalue and eigenfunction problems); dynamics plays a minor role (problems on the radiation–atom interaction and particle scattering). Meanwhile, it is quantum dynamics that prevails in contemporary quantum systems research, as is clear from the presentation of the theory of quantum information systems. It is supposedly expedient to construct a modern course in quantum mechanics such that it consists of two full-fledged volumes dedicated to quantum statics and quantum dynamics. It is believed that such a course on quantum mechanics will make its appearance in the near future.

References

1. Dowling J P, Milburn G J, quant-ph/0206091
2. Boto A N et al. *Phys. Rev. Lett.* **85** 2733 (2000)
3. Bennett C H, Brassard G, in *Proc. of the Intern. IEEE Conf. on Computers, Systems and Signal Processing, Bangalore, India, 1984* (New York: IEEE Press, 1984) p. 175
4. Dowling J P *Phys. Rev. A* **57** 4736 (1998)
5. Wineland D J et al. *Rev. Mod. Phys.* **71** 253 (1999)
6. Nägerl H C et al. *Phys. Rev. A* **60** 145 (1999)
7. Kane B E *Nature* **393** 133 (1998)
8. Ekert A, Hayden P, Inamori H, quant-ph/0011013
9. Shor P W, in *Proc. of the 35th Annual Symp. on the Foundation of Computer Science, Los Alamitos, CA, USA* (New York: IEEE Press, 1994) p. 124
10. Plenio M B, Vitelli V *Contemp. Phys.* **42** 25 (2001); quant-ph/0103108
11. Makhlin Y, Schön G, Shnirman A *Rev. Mod. Phys.* **73** 357 (2001)
12. Nakamura Y, Pashkin Yu A, Tsai J S *Nature* **398** 786 (1999)
13. Orlando T P et al. *Phys. Rev. B* **60** 15398 (1999)
14. Bouwmeester D, Ekert A K, Zeilinger A (Eds) *The Physics of Quantum Information* (Berlin: Springer, 2000)
15. Nielsen M A, Chuang I L *Quantum Computation and Quantum Information* (Cambridge: Cambridge Univ. Press, 2000)
16. Hardy L, quant-ph/0101012; de Muynch W M, quant-ph/0307235
17. Pradhan P et al., quant-ph/0402122
18. Galvao E F, Ph.D. Thesis (Oxford: Univ. of Oxford, 2002); quant-ph/0212124
19. Landau L D, Lifshitz E M *Kvantovaya Mekhanika. Nerelyativistskaya Teoriya* (Quantum Mechanics: Non-Relativistic Theory) (Moscow: Fizmatgiz, 1963) [Translated into English (Oxford: Pergamon Press, 1977)]
20. Schrödinger E *Naturwissenschaften* **23** 807 (1935)
21. Einstein A, Podolsky B, Rosen N *Phys. Rev.* **47** 777 (1935)
22. Ghirardi G C, Marinatto L *Phys. Rev. A* **70** 012109 (2004); quant-ph/0401065
23. Dür W, Vidal G, Cirac J I *Phys. Rev. A* **62** 062314 (2000)
24. Coffman V, Kundu J, Wootters W K *Phys. Rev. A* **61** 052306 (2000)
25. Vandersypen L M K, Ph.D. Thesis (Stanford, Calif.: Stanford Univ., 2001); quant-ph/0205193
26. Klyshko D N *Fotony i Nelineĭnaya Optika* (Photons and Nonlinear Optics) (Moscow: Nauka, 1980) [Translated into English (New York: Gordon and Breach, 1988)]
27. Mandel L, Wolf E *Optical Coherence and Quantum Optics* (Cambridge: Cambridge Univ. Press, 1995) [Translated into Russian (Moscow: Fizmatlit, 2000)]
28. Mamin H J et al. *Phys. Rev. Lett.* **91** 207604 (2003)
29. Devoret M H, Schoelkopf R J *Nature* **406** 1039 (2000); Kane B E et al. *Phys. Rev. B* **61** 2961 (2000)
30. Kokin A A, Valiev K A, quant-ph/0201083; quant-ph/0306005
31. Lupascu A et al. *Phys. Rev. Lett.* **93** 177006 (2004); cond-mat/0311510
32. Vion D et al. *Science* **296** 886 (2002); cond-mat/0205343
33. Grover L, in *Proc. of the 28th Annual ACM Symp. on Theory of Computation* (New York: ACM Press, 1996) p. 212
34. Manin Yu I *Vychislimoe i Nevychislimoe* (Computable and Non-computable) (Moscow: Sov. Radio, 1980)
35. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
36. Abrams D S, Lloyd S *Phys. Rev. Lett.* **79** 2586 (1997)
37. Kempe J, Shalev A, quant-ph/0406046
38. Bennett C H et al. *Phys. Rev. Lett.* **70** 1895 (1993); Yimsiriwattana A, Lomonaco S J (Jr), quant-ph/0402148
39. Abrams D S, Lloyd S *Phys. Rev. Lett.* **83** 5162 (1999)
40. Cheng Y C, Silbey R J, quant-ph/0312053; *Phys. Rev. A* (submitted)
41. Ekert A, Macchiavello C *Acta Phys. Pol. A* **93** 63 (1998); quant-ph/9904070
42. McConnell J *The Theory of Nuclear Magnetic Relaxation in Liquids* (Cambridge: Cambridge Univ. Press, 1987)
43. Georgeot B, Shepelyansky D L, quant-ph/9909074
44. Wineland D J et al. *J. Res. Natl. Inst. Stand. Tech.* **103** (3) 259 (1998)
45. Byrd M S, Wu L-A, Lidar D A, quant-ph/0402098
46. Abbott D, quant-ph/0310130
47. Thorwart M, Hänggi P *Phys. Rev. A* **65** 012309 (2002)
48. Palma G M, Suominen K-A, Ekert A K *Proc. R. Soc. London Ser. A* **452** 567 (1996); quant-ph/9702001
49. Bennett C H et al. *Phys. Rev. A* **54** 3824 (1996)
50. Steane A M *Phys. Rev. Lett.* **77** 793 (1996)
51. Shor P W, quant-ph/9605011
52. Steane A M, quant-ph/0207119
53. Bacon D, Brown K R, Whaley K B *Phys. Rev. Lett.* **87** 247902 (2001); quant-ph/0012018
54. Vaidman L, Goldenberg L, Wiesner S *Phys. Rev. A* **54** R1745 (1996)
55. Erez N et al., quant-ph/0309162
56. Facchi P, Lidar D A, Pascazio S *Phys. Rev. A* **69** 032314 (2004); quant-ph/0303132
57. Hotta M, Morikawa M, quant-ph/0401164
58. Facchi P, Nakazato N, Pascazio S *Phys. Rev. Lett.* **86** 2699 (2001)
59. Tasaki S et al. *Int. J. Quantum Chem.* **98** 160 (2004); quant-ph/0210129
60. Viola L, Lloyd S *Phys. Rev. A* **58** 2733 (1998)
61. Ahn C, Wiseman H M, Milburn G J *Phys. Rev. A* **67** 052310 (2003)
62. Sarovar M et al. *Phys. Rev. A* **69** 052324 (2004); quant-ph/0402017
63. Ahn C, Doherty A C, Landahl A J *Phys. Rev. A* **65** 042301 (2002)
64. Vedral V, quant-ph/0212133
65. Berry M V *Proc. R. Soc. London Ser. A* **329** 45 (1984)
66. Freedman M H et al. *Bull. Am. Mat. Soc.* **40** 31 (2002)
67. Unanyan R G, Shore B W, Bergmann K *Phys. Rev. A* **59** 2910 (1999)
68. Byrd M S, Lidar D A *J. Mod. Opt.* **50** 1285 (2003); quant-ph/0210072
69. Kielpinski D, Monroe C, Wineland D J *Nature* **417** 709 (2002); Cirac J I, Zoller P *Nature* **404** 579 (2000)
70. Loss D, DiVincenzo D P *Phys. Rev. A* **57** 120 (1998); Hollenberg L C L et al., cond-mat/0306235

71. Makhlin Yu, Schön G, Shnirman A *Rev. Mod. Phys.* **73** 357 (2001); cond-mat/0011269
72. Dowling J P et al., quant-ph/0402090; Pittman T B, Jacobs B C, Franson J D, quant-ph/0406192; quant-ph/0404059
73. Cirac J I, Duan L M, Zoller P, quant-ph/0405030
74. Dykman M I, Platzman P M, quant-ph/0109030
75. Brennen G K, Deutsch I H, Jessen P S, quant-ph/9910031
76. Kokin A A, quant-ph/0002034; Benjamin S C, Bose S, quant-ph/0210157
77. Cornell E A, Wieman C E *Rev. Mod. Phys.* **74** 875 (2002); *Usp. Fiz. Nauk* **173** 1320 (2003); Ketterle W *Rev. Mod. Phys.* **74** 1131 (2002); *Usp. Fiz. Nauk* **173** 1339 (2003)