Using quantum computing to create efficient algorithms

I N Balaba\textsuperscript{1}, G S Deryabina\textsuperscript{2}, I A Pinchuk\textsuperscript{3}, I V Sergeev\textsuperscript{4} and S B Zabelina\textsuperscript{3}

\textsuperscript{1}Tula State Lev Tolstoy Pedagogical University, 300026, Tula, Lenin avenue, 125, Russia
\textsuperscript{2}Bauman Moscow State Technical University, 105005, Moscow, ul. Baumanskaya 2-ya, 5, Russia
\textsuperscript{3}Moscow Region State University, 141014, Moscow Region, city of Mytishi Very Voloshinoy street, 24, Russia
\textsuperscript{4}Institute of Advanced Training and Professional Retraining of Educational Workers Tula region, 300041, Tula, Lenin street, 22, Russia

Corresponding author: irenepin@yandex.ru

Abstract. The article presents a historical overview of the development of the mathematical idea of a quantum computing model - a new computational strategy based on the postulates of quantum mechanics and having advantages over the traditional computational model based on the Turing machine; clarified the features of the operation of multi-qubit quantum systems, which ensure the creation of efficient algorithms; the principles of quantum computing are outlined and a number of efficient quantum algorithms are described that allow solving the problem of exponential growth of the complexity of certain problems.

1. Introduction
The need to build quantum computations (quantum algorithms) is due to the need to solve a wide range of computational problems for which there are no efficient classical (polynomial) algorithms. Inefficient algorithms require exponentially large resources that even supercomputers cannot provide. At the same time, quantum computing, using the paradigm of quantum mechanics, allows you to solve these problems. Quantum computers are needed to solve such problems.

The idea of creating quantum computers began to be discussed back in the 60s of the XX century. By this time, quantum statistical mechanics and quantum field theory already existed. J. Von Neumann's works laid a solid mathematical foundation for the statistical interpretation of quantum mechanics. L.D. Landau was the first to point out the possibility of describing a system by a density matrix [1]. A little later, von Neumann published two articles in which, using the density matrix, he gave a very complete analysis of issues related to the probabilistic interpretation of quantum mechanics and thermodynamics of quantum mechanical systems [2, 3].

In 1980, Yu. I. Manin noted that quantum computers can simulate quantum systems more efficiently than classical computers could. He believed that one of the reasons for this is that the quantum state space of a quantum automaton has a much greater capacity than the classical one: where in the classics there are \( N \) discrete states, in the quantum theory admitting their superposition, there are \( C^N \) Plank states of the cells. When combining classical systems with the number of states \( N_1 \) and \( N_2 \),...
the total number of states will be equal to the product $N_1 \cdot N_2$, and in the quantum version we will get $C^{N_1 \cdot N_2}$ [4, page 15].

In 1982, the idea was developed in more detail by R.P. Feynman in [5], in which he noted that modeling quantum mechanical systems is an exponentially difficult task for classical computers, but can be effectively carried out by performing logical operations on quantum systems, acting on superposition of many quantum states.

In 1985, D. Deutsch developed the concept of a quantum computer and showed how quantum computers could be built from quantum logic gates in quantum networks, from which it followed that a quantum computer could indeed surpass classical computers in computational efficiency.

At the beginning of the 21st century, a monograph by American specialists M. Nielsen and I. Chang [6] was published, which sets out the main results in the field of quantum computing and quantum informatics in sufficient completeness and scientific rigor.

2. Quantum computers

The main element of a quantum computer is quantum bits (qubits), lists of quantum states. This is their difference from modern classical computers, in which bits are used to transfer and process data, each of which at any time can be in one of two states 0 or 1. An arbitrary qubit $|\psi\rangle$ admits two classical states, denoted $|0\rangle$ and $|1\rangle$, but it can also be in their superposition (linear combination), that is, in the state $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, where $\alpha$ and $\beta$ are complex numbers satisfying the condition $|\alpha|^2 + |\beta|^2 = 1$, and $|\alpha|^2$ and $|\beta|^2$ are respectively the probability of getting 0 or 1 when measuring the state of a qubit.

Since each qubit can be in a superposition of the states $|0\rangle$ and $|1\rangle$, the state space of a system constructed from only two qubits $|\phi\rangle, |\psi\rangle$, is a superposition of four basic states $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$, which is much "more" than the only possible state of a system built of two classical bits at each moment in time. If a classical computer stores $N$ bits in memory, which are subject to change for each cycle of the processor's operation, then a quantum system of $N$ two-level quantum elements has $2^N$ linearly independent states. Hence, due to the principle of quantum superposition, the state space of a quantum system is a $2^N$-dimensional Hilbert space, the standard basis of which is a unit matrix of size $2^N \times 2^N$. Of course, there can be an infinite number of bases, but all vectors are orthonormal. One operation on a group of qubits affects all the values that it can take, in contrast to the classical bit, which provides unprecedented parallelism of computations, an exponential increase in the power of the computational model.

Quantum circuit is a model of quantum computing that serves to visualize quantum algorithms (Figure 1).

![quantum circuit](image-url)

**Figure 1.** An example of a quantum circuit that uses two qubits.

A quantum scheme is represented in $2^N$-dimensional Hilbert space, where $N$ is the number of qubits, and each unitary transformation is a matrix of a special form.

Building a quantum automaton requires the right balance between mathematical and physical principles. To create a quantum computer, it is necessary to simulate its operation on the basis of real physical systems, taking into account quantum noise, which is the main problem on the way of implementing quantum bits. The physical realization of a qubit can be any two-level quantum mechanical system, for example, polarization states of photons or spin states of atomic nuclei. The following requirements are imposed on them:

- the system consists of a precisely known number of particles;
- the ability to bring the system to a precisely known initial state;
- a high degree of isolation from the external environment;
- providing measurements with a sufficiently high reliability of the state of the quantum system at the output.

When creating a quantum computer, the main attention is paid to the issues of controlling qubits using stimulated emission and preventing spontaneous emission, which will disrupt the operation of the entire quantum system. The main technical obstacle to creating a quantum computer with a sufficient number of qubits is decoherence - the decay of quantum superpositions. Random interactions with objects in the surrounding world can destroy the state in which the qubits are located and break the connections between them. For many years, research has been underway to extend the lifetime of qubits by isolating them from the environment in various ways. In 2020, an approach was developed to solve the problem of decoherence of superconducting qubits based on Josephson transitions [7].

3. Principles underlying quantum computing
The physical foundations of quantum computing are the postulates of quantum mechanics. Let us recall them.

1. The state of an isolated quantum system is described by the unit vector of a complex Hilbert space. The state of a quantum bit in a 2-dimensional complex Hilbert space is described by a unit vector:

$$|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle, |\alpha|^2 + |\beta|^2 = 1,$$

where $\alpha$ and $\beta$ are complex numbers.

2. The evolution of a closed quantum system is described by the unitary operator $U$.

3. The state space of a composite system is the tensor product of the state spaces of the systems included in it.

4. Quantum measurements are described by a set of operators $\{M_m\}$, acting on the state space of the system. If the state of the system before the measurement is $|\psi\rangle$, then the probability of obtaining the result $m$ is

$$P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle,$$

where $M_m^\dagger$ is the Hermitian-conjugate matrix to $M_m$ and the state of the system after measurement:

$$|\psi\rangle \rightarrow \sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle} M_m |\psi\rangle.$$

Measurement operators satisfy the completeness equation:

$$\sum_m M_m^\dagger M_m = I.$$

Quantum computing is based on the following principles:

1. Reversibility of calculations, i.e. any computational process within the framework of quantum computing must be reversible. This means that for any quantum circuit underlying the algorithm, it is possible to build a reverse circuit, which, receiving the output of the original circuit as input, returns the initial data for it.

2. Quantum parallelism. Since the quantum bit can be either 0 or 1, then by calculating some function, the argument of which is set by quantum bits, all possible values are calculated simultaneously. This makes it possible to solve the same problem in parallel for exponentially big data.

3. Interference is widely used in quantum algorithms to enhance desired results and attenuate unwanted ones. Repeating several times the sequence of parallel processing of qubits, taking into account the interference of their states, it is possible to obtain the required result with a high probability. In this case, by varying the number of repetitions and the step of interference, the probability can be brought to any given value.
4. Quantum entanglement is the most important property of quantum systems. It serves as an essential resource in quantum informatics, being a key factor in many quantum algorithms.

The main specific feature of quantum computing is its probabilistic nature. In [8], the authors considered the development of the use of probabilistic methods in theoretical physics from the kinetic theory of gases to the Einstein – Podolsky – Rosen paradox and Bell inequalities.

4. Quantum algorithms

When developing quantum algorithms, of greatest interest are those that are fundamentally superior to classical algorithms in speed.

An outstanding result in this direction was obtained by Shor [9]. He found two polynomial quantum algorithms for which no classical analogs were known. The first is an algorithm for factoring an integer into a product of prime factors (factoring of integers), and the second (the discrete logarithm) is an algorithm for solving the equation \( a^d = b \) for given elements \( a \) and \( b \) in a finite abelian group \( G \). Shor's factorization algorithm, allowing to factor the number \( N \) into prime factors in time \( O(\log^3 N) \) is based on the ability of qubits to take several values simultaneously. This algorithm consists of two parts: the classical first is the reduction of the factorization to finding the period of some function, the quantum second is the finding of the period of this function. Shor's factorization algorithm is quite simple and requires more modest hardware than a general-purpose quantum computer. And since numerous modern algorithms and cryptography systems are based on the algorithmic complexity of the problem of factorizing a number, it makes it possible to hack public key cryptographic systems, in particular the RSA cryptosystem, with its help.

A. Yu. Kitaev formulated and solved the Abelian Stabilizer Problem, which includes the above algorithms as special cases [10]. This problem is as follows. Let a finite abelian group \( G \) act on a finite set \( M \). It is assumed that this action and the group operation are easily computable. We need to find a stabilizer for an element \( a \) of a group \( G \), that is, find a subgroup \( H \) of a group \( G \) that leaves the element \( a \) in place.

In turn, a generalization of the Abelian stabilizer problem is the Hidden Subgroup Problem. This problem remains one of the fundamental problems in the theory of quantum algorithms. It is formulated as follows. Let a function \( f : G \rightarrow S \) be given with the following property: it is constant on the cosets of the group \( G \) with respect to the subgroup \( H \) and different on different cosets. The difficulty of solving this problem depends on the properties of the group \( G \). In recent years, an efficient algorithm has been found in the case when \( H \) is a normal subgroup of the group \( G \) [11]. An efficient algorithm was constructed for a group \( G \) that is close to Abelian, that is, one for which the intersection of all normalizers of subgroups has a small index in the group \( G \) [12]. A beautiful solution was also found in the class of nilpotent groups of degree 2 [13].

It should be noted that the problems of automorphism and isomorphism of graphs can be formulated in the language of the hidden subgroup problem for the symmetric group \( S_n \).

The key role in quantum computing is played by the Fourier transform, which, if written appropriately, can significantly increase the efficiency of computations. If the input for the Fourier transform is an \( N \)-dimensional vector, then the classical algorithm requires \( O(N \log N) \) operations, and the quantum one requires \( O(\log^2 N) \) operations. In many problems, the Fourier transform was defined on the set of a sequence of complex numbers \( \{a_g\} \), where \( g \in \mathbb{Z}_{2^n} \). Kitaev in [10] generalized the Fourier transform from \( \mathbb{Z}_{2^n} \) to the Fourier transform on an arbitrary finite abelian group.

In 1996, L. Grover developed a quantum algorithm that allows searching in any unordered database of \( N \) elements in \( O(\sqrt{N}) \) time [14]. Currently, one of the fastest search algorithms is the linear algorithm, which requires \( O(N) \) time. Grover's algorithm is the fastest quantum algorithm for searching in an unordered database, and there are no classical algorithms with the same efficiency.

At the moment, several dozen quantum algorithms have been developed in the world for solving various problems.
Note that quantum computers could not only efficiently solve exponentially complex traditional mathematical problems, but also a whole class of new problems that no classical computer can solve. In 1984 Bennett and Brassard [15] developed the first quantum cryptography algorithm based on the quantum state of photons. In 1989, the first working quantum computer was built at the IBM Research Center, consisting of two quantum cryptographic devices, implementing a system of quantum cryptography. The secrecy of the system is based not on the difficulty of processing, but on the properties of quantum interference, which gives this system absolute secrecy, which cannot be ensured using classical methods [16, p. 221]. Further improvement of the cryptosystem reliability was proposed by A. Eckert, based on the Einstein-Podolsky-Rosen effect [17].

5. Conclusions
Full-fledged quantum computers have not yet been created; only their prototypes exist, which are implemented using various technologies for creating a quantum environment. In November 2009, a programmable quantum processor model was created. Physicists from the National Institute of Standards and Technology (USA) have implemented an extensive set of "programs" based on two qubits, represented by beryllium ions. In January 2010, a primitive quantum computer was used to calculate the energy of a hydrogen molecule. Physicists from Harvard University (USA) and the University of Queensland (Australia) managed to implement an algorithm for calculating the energy of the ground and excited states of the H2 molecule, using only two photon qubits in their experiments. Institute for Theoretical Physics Landau RAS and the RAS Physico-Technological Institute conduct experiments with different architectures of quantum computers and with different materials. In April 2012, a team of researchers from the University of Southern California, Delft University of Technology, Iowa State University, and the University of California managed to build a two-qubit quantum computer based on an impurity diamond crystal. It implements Grover's algorithm for 4 iteration options. In 2019, Google announced the creation of a 53-qubit Sycamore prototype, which uses superconducting qubits.

It remains relevant to simulate the operation of a quantum computer on classical supercomputers, since when simulating a quantum computer on a classical computer, the amount of required computing resources exponentially increases with the number of qubits. The work [18] presents a simulation of the operation of an ideal quantum computer on the Lomonosov supercomputer. The authors have developed special software that simulates the Grover quantum algorithm and the quantum Fourier transform.

The current stage in the development of quantum computing is the stage of fundamental research and experimental confirmation of the results of these studies.

Acknowledgements
The work of I N Balaba was supported by the RFBR grant No 19-41-710004_r_a

References
[1] Landau L 1927 Zeitschrift für Physik 45 430
[2] von Neumann J 1927 Nachr. Akad. Wiss. Göttingen Math.-Phys 245
[3] von Neumann J 1927 Nachr. Akad. Wiss. Göttingen Math.-Phys 273
[4] Manin Y 1980 Computable and uncomputable (Moscow, Sovetskoe radio) 128 (in Russ.)
[5] Feynman R P 1982 Int. J. Theor. Phys 21 467
[6] Nielsen M A and Chuang I L 2000 Quantum computation and quantum information (Cambridge University Press) 704
[7] Bilmes A, Volosheniuk S, Brehm J D, Ustinov A V and Lisenfeld J 2020 Quantum Sensors for Microscopic Tunneling Systems arXiv:2011.14327v1
[8] Deryabina G S, Kuleshova Ju D, Pinchuk I A, Zabelina S B and Vysotskaya P A 2020 J. Phys.: Conf. Ser. 1560 012013
[9] Shor P 1994 *Foundations of Computer Science, Proceedings., 35th Annual Symposium on* (IEEE) 124
[10] Kitaev A Yu 1995 *Quantum measurements and the Abelian stabilizer problem* (arXiv:quant-ph/9511026v1)
[11] Hallgren S, Rassell A and Ta-Shma A 2003 *SIAM Journal on Computing* 32(4) 916
[12] Gringi M, Schulman L, Vazirani M, and Vazirani U 2004 *Combinatorica* 24(1) 137
[13] Ivanyons G, Sanselme L, and Santha M 2012 *Algorithmica*, 62(1-2) 480
[14] Grover L.K. 1996 *Proceedings, 28th Annual ACM Symposium on the Theory of Computing* 212.
[15] Bennett C H, Brassard G 1984, *Proceedings of the Intern. IEEE Conf. on Computers, Systems and Signal Processing, Bangalore, India,* (New York: IEEE Press) 175
[16] Deutsch D 1997 *The fabric of reality* London: Allen Lane) 390
[17] Ekert A 1991 *Phys. Rev. Lett.* 67 661
[18] Andreev D Yu, Korzh O V, Korobkov S V and Chernyavsky A Yu 2013 *Proc. Int. Conf. Parallel computational technologies (PCT) 2013* (Chelyabinsk: Publishing Center SUSU) 38