УДК 811.111:519.68

Baskov A., Soroka S., Beznis Y.

**Quantum Computer**

Belarusian National Technical University
Minsk, Belarus

Digital electronic computers widely used today are created using semiconductor technologies. Such computers are usually a collection of elements with only two possible logical states "0" and "1" – the so-called "bits". Such computers, in which logical operations are performed with these classical (from the point of view of physics) states are now commonly called classical. However, these classical computers cannot cope with some very important tasks. Examples of such tasks include searching in an unstructured database, modeling the evolution of quantum systems (for example, nuclear reactions), and finally factorizing large numbers.

The idea of quantum computing was first expressed by Yu. I. Manin in 1980 [1], but this problem was actively discussed after the appearance of an article by the American theoretical physicist R. Feynman in 1982 [2]. In these works, it was proposed to use operations with states of a quantum system for calculations. The authors drew attention to the fact that each state of a quantum system, in contrast to the classical one, can be in a superposition state. In terms of a classical computer, a quantum bit, or qubit, can be in the "0" and "1" states simultaneously, according to the laws of quantum mechanics. The most popular attempt to explain this "strangeness" of the quantum world is made on the example of the electron spin property, which is clearly manifested in nuclear magnetic resonance (NMR) experiments.

Currently, a new class of quantum devices – quantum computers – is being developed. Strictly speaking, there are two types of quantum computers. Both are based on quantum phenomena, but of a different order. Representatives of the first type are, for example, computers based on quantization of magnetic flux based on superconductivity violations - Josephson transitions. The Josephson effect is already used for linear amplifiers, analog-to-digital converters, squids, and correlators. A project for creating a RISC processor based on RSFQ (Rapid Single Flux Quantum) logic is known. The same element base is used in the project to create a petaflop (1015 op. / from the computer). A clock frequency of 370 GHz has been experimentally achieved, which can be further increased to 700 GHz. However, the time of defocusing wave functions in these devices is comparable to the time of switching individual gates, and in fact the already familiar element base – triggers, registers, and other logical elements – is implemented on new, quantum principles [3].

Another type of quantum computers, also called quantum coherent computers, requires maintaining the coherence of the wave functions of qubits used throughout the calculated time – from beginning to end (a qubit can be any quantum mechanical system with two separate energy levels). As a result, for some problems, the computational power of coherent quantum computers is proportional to 2N, where N is the number of qubits in the computer. It is the latter type of device that is implied when we talk about quantum computers.

A classical computer consists, roughly speaking, of a certain number of bits that can be used to perform arithmetic operations. The main element of a quantum computer (QC) is quantum bits, or qubits (from Quantum Bit, qubit). A normal bit is a classical system that has only two possible states. We can say that the bit space of states is a set of two elements, for example, zero and one. A qubit is a quantum system with two

possible states. There are a number of examples of such quantum systems: an electron whose spin can be either +1/2 or -1/2, atoms in a crystal lattice under certain conditions. But since the system is quantum, its state space will be incomparably richer. Mathematically, a qubit is a two-dimensional complex space.

In such a system, you can perform unitary transformations of the system's state space. From the point of view of geometry, such transformations are a direct analog of the rotation and symmetry of ordinary three-dimensional space. According to the superposition principle, you can add states, subtract them, and multiply them by complex numbers. These states form a phase space. When two systems are combined, the resulting phase space will be their tensor product. The evolution of the system in the phase space is described by unitary transformations of the phase space [3].

There are two examples of non-trivial problems in which QC gives a radical gain. The first of them is the problem of decomposing integers into prime factors and, as a result, calculating the discrete logarithm (DL). A prime number has primitive roots – such deductions whose degrees generate all non-zero elements. If such a root is given and the degree is given, then you can quickly raise it to a power (for example, first we square it, then we get the fourth power, and so on). The DL is the inverse problem. Given a primitive root and some element of the field; find the degree to which you need to raise this root to get this element. This task is already considered difficult. So complex that several modern cryptographic systems assume that it is impossible to calculate the DL in an acceptable time if the module is a sufficiently large. So, for a discrete logarithm, there is an efficient quantum algorithm [4].

So far, quantum computers can only handle the simplest tasks – for example, they are already able to add 1 and 1, resulting in 2. It was also planned to take another important

milestone – the factorization of the number 15, it will be decomposed into Prime factors – 3 and 5. And then, you may see, it will come to more serious tasks.

Prototypes now contain less than ten quantum bits. According to Neil Gershenfeld who participated in the creation of one of the first working models of a quantum computer, it is necessary to combine at least 50-100 qubits to solve problems that are useful from a practical point of view. Interestingly, adding each subsequent qubit to a quantum computer based on the effect of volumetric spin resonance requires increasing the sensitivity of the equipment twice. Ten additional qubits will thus require a sensitivity increase of 1000 times, or 60 dB [4].

Highly possible that the advent of the quantum computer in the information society will play the same role as the invention of the atomic bomb in the industrial society. Indeed, if the latter is a means of "destroying matter", then the former can become a means of "destroying information" – because very often what everyone knows is not necessary for anyone.

References:

1. Manin, Yu. I. Computable and non-computable. – Moscow: Soviet radio, 1980. – 128 p.
2. R. Feynman. Quantum mechanical computers. – Originally in Optics News, 1985. –11-20 p.
3. [Electronic resource]. – Mode of access: https://en.wikipedia.org/wiki/Symmetry_in_quantum_mechanics. – Date of access: 23.03.2020.
[Electronic resource]. – Mod of access: https://www.technologyreview.com/2003/03/01/101907/harnessing-quantum-bits/.