УДК 004.415.3:681.6

M. Alekseyev[1], O. Syrotkina[2], S. Kostrytska[1], E. Zyabrieva[1]
[1]Dnipro University of Technology, Dnipro, Ukraine
[2]School of Computer Science University of Windsor, Windsor, Ontario, Canada

THE QUANTUM COMPUTER POTENTIAL

Abstract. The efficient system architecture of quantum computers has led to improvements in various areas. This paper describes the concepts of quantum computing and quantum computing applications. The current status of the developments in quantum computing is presented.

Keywords: *qubits, laws of quantum mechanics, state of "superposition", interference, entanglement, quantum computers, basic database, modeling of quantum systems.*

Introduction. Nowadays, modern processes are based on the principle of the binary system. Some people believe that with the correct organization of transistors and logic circuits, you can do almost anything. In fact, modern computers are not all-powerful. For example, if we are talking about big data, ordinary computers can take years or even thousands of years to process data, calculate the desired option and give the result, unlike quantum computers. This research is about the structure and features of quantum computers.

Quantum algorithms manipulate related qubits in their uncertain state (the "superposition" state), potentially providing the ability to solve problems of enormous combinatorial complexity. The purpose of the study is to describe the quantum computer operating principle and to outline the future of this invention.

Formulation of the task. To achieve the aim of the study, the following tasks were set:

- to analyze the architecture of the system;
- to define the advantages and disadvantages of the system;
- to delineate what the complexity of the work may be;
- to single out what awaits us thanks to this invention.

The most powerful FUGAKU computer is given a seemingly elementary task: to seat 3 students in 2 places. The number of possible options will be two in the third degree. The computer calculates this in seconds, but if you complicate the task a bit (you need to place 100 students in 2 places), this calculation will take more time than the summed lives of hundreds of universes ($\pm$ 4.6 * 10^{35} years). However, quantum computers solve this problem in seconds. This happens because quantum computers have different architecture.

Classic processor consists of transistors. They can either pass current (be in state 1) or not pass current (be in state 0), i.e. this is a bit of information (fig.1).

Returning to our example, everyone can be either in place (state 1) or out of place (state 0). To solve the problem, the processor needs to review all the options and select the ones that meet the condition. Quantum computers use quantum bits (qubits), which are fundamentally different.

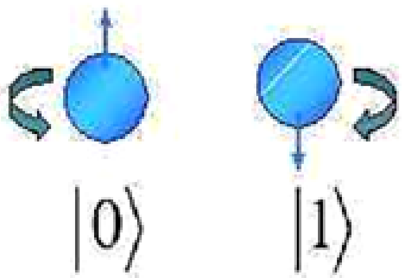

Fig. 1. Classic bit

The increase in the speed of work is due to three phenomena of quantum mechanics: superposition, interference, entanglement.

The qubit can also take values 0 and 1, but, unlike a simple bit, it is not limited to them. If a qubit can be in two basis states, it can also be in the superposition of these states, i.e. it can take many intermediate values. For example, in quantum calculations, it is possible that the qubit is in the $|0\rangle$ state with a probability of, say, 0.9, and in the $|1\rangle$ state with a probability of 0.1. It is known from probability theory that the sum of the probabilities of finding the system of a finite set of states is always equal to 1 (or 100%). If the sum of the probabilities is less, it means that some conditions are not taken into account [1].

It is convenient to represent the space of qubit states as Bloch spheres. At the north pole of the sphere the values are 0, at the south - 1, which in turn can denote the spins of the electron ("spin up" and "spin down"), but there is also the rest of the surface, that illustrate all sorts of states (fig. 2).

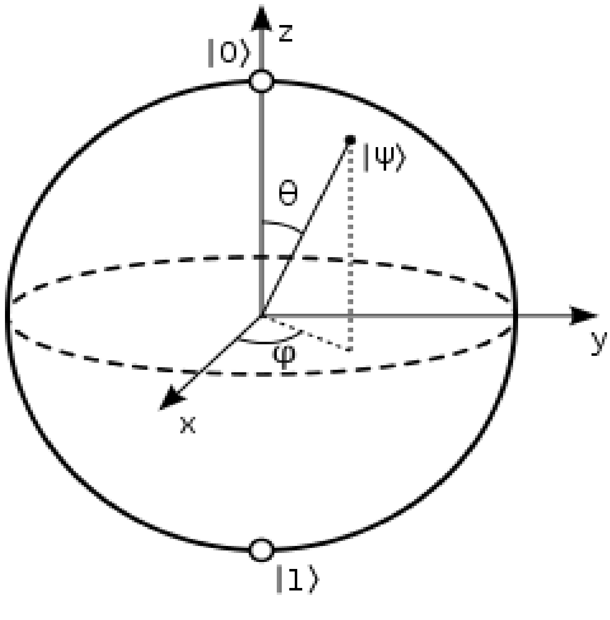

Fig. 2. Bloch sphere (adapted from [1])

Quantum object (in our case, a qubit) is in "superposition" until you change it. For example, if we toss a coin, it is both heads and tails in flight until someone catches it.

Due to the superposition, the qubits can have a value of 1, or 0, or an intermediate value. Depending on the configuration, the qubit has a certain probability of collapsing to 1 or 0. This probability of collapse into one or another state is determined by quantum interference. Moreover, if an event, for example, a photon crashing into a point on the screen, can occur in one case with a positive amplitude and in another case with a negative one, then both probabilities can be mutually destroyed. The total amplitude will be zero and the event will never happen. This phenomenon is called quantum interference [2].

Qubit is simply a quantum bit of information with two probability amplitudes. If you observe a qubit, you randomly force it to take a value of either 0 or 1. However, if you do not observe it, the amplitudes interfere and the qubit produces effects inherent in both amplitudes [2].

Quantum interference affects the state of the qubit to affect the probability of obtaining a certain result during the measurement. This probabilistic nature makes quantum computing very powerful [2].

Entangled qubits form a single system and affect each other. By measuring the state of one qubit, we can conclude about others. As the number of entangled qubits increases, the ability of quantum computers to process information increases exponentially. Due to this interdependence, particles can maintain communication, even when separated by incredibly long distances [1].

However, qubits are quite unstable. People have not yet decided which quantum objects are best to use. There are many options. It can be electrons or photons. Quantum qubits in physical realization also come in several types: superconductors, charge, ion traps, quantum dots, and others. Historically, superconductors were considered to be the most promising direction due to good scalability, stability over time, control of parameters and relative ease of management. International Business Machines Corporation (IBM), Google and Rigetti quantum computers are built on this platform. However, alternative quantum platforms have recently become increasingly popular: ions, which demonstrate the highest stability and accuracy of operations (Honeywell, IonQ), and photons, the advantages of which are small photon processor size and the ability to work at room temperature (PsiQuantum, Quix).

The level of current technological development allows to create a large number of qubits. The difficulty arises with the stability of such a system. Like all quantum systems, qubits easily lose a given quantum state when interacting with the environment (their decoherence occurs). As a result, the number of computational errors in the quantum computer increases. To ensure its stability during calculations, you need to protect the system from any background noise, for example, in the case of superconducting systems, cooling them to temperatures close to zero Kelvin (-273.1 ° C). The developers use superfluid liquids to achieve such cooling.

Returning to the problem from the example, the classical computer has to go through all possible options, but since the qubit is 1 or 0 or an intermediate value, the quantum computer goes through all the options at the same time. Then, you need a certain mathematical operator, such as a grover, to recognize the correct option, and this requires quantum algorithms.

The most famous quantum algorithms can be divided into three [3]:

- Shora (decomposition of numbers into prime factors);
- Grover (quick search in an unordered database);
- Deutsch–Jozsa (answer to the question if the function is constant and acquires either value 0 or value 1 for any argument, or balanced acquring for half of the domain value 1, for the other half value 0);

There are a lot of tasks for quantum computers in the near future. They will become the main database. The search for it will be faster because he principle of superposition, in which the basic unit of information can exist in more than one state at a time, allows a quantum computer to store and process much more data than any other computer. Shazam will be incredibly fast.

Quantum systems can be used to solve the problem of the salesman, a task that requires the shortest route between many cities before returning home. Solving this problem would allow better construction of navigation and route planning around the world, which would reduce the cost and simplify the movement of people and goods. Volkswagen is already conducting a similar study with D-Wave and Google.

Neural networks and artificial intelligence will get an incredible boost. Features of quantum computing, such as quantum parallelism or the effects of interference and confusion can be used as starting points. However, since the technological implementation of the quantum computer is still premature, such models of the quantum neural network are mostly theoretical proposals that await their implementation in physical experiments.

In addition, modeling of quantum systems will appear. This is very important because it will thus be possible to build models of the interaction of complex protein compounds. Such "quantum chemistry" is so complex that only the simplest molecules can be analyzed with the help of modern digital computers.

Chemical reactions are quantum in nature, as they form rather confusing quantum states of superposition. Highly developed quantum computers can easily calculate complex processes. This will be very important for medicine, opening up stunning oportunities to create future medicines and to understand how different viruses, like covid-19, affect us.

Quantum computers are used to develop cryptographic techniques. In August 2015, the National Security Agency (NSA) began compiling a list of quantum-resistant cryptographic methods that could withstand quantum computers [4]. In April 2016, US National Institute of Standards and Technology began a process of evolution, which will last for 4-6 years [4].

Promising methods of quantum encryption, which involve the one-sided nature of quantum entanglement, are also under development [4].

Another advantage of quantum computers is that financial transactions such as arbitrage can require consecutive steps, and the number of ways to calculate them far exceeds the number allowed for a conventional digital computer.

Quantum computers are being developed by Google, Intel, Microsoft and other companies.

Microsoft is working with quantum computing equipment companies to give developers the cloud access to quantum computers. Using the Azure Quantum platform and the Q # language, developers will be able to explore quantum algorithms and run their quantum programs on various types of quantum computing equipment.

In addition, every major institute has research teams working on the development and research of quantum computers, so it is now a matter of several years before the quantum computers begin to be used everywhere.

The American technology company IBM announced that it has developed a new chip for quantum computing, which will allow quantum systems to surpass classic computers in some tasks over the next two years. Its new Eagle chip has 127 qubits, making it the world's most productive quantum processor [4].

In 2022, the company also intends to release the quantum chips Osprey with 433 qubits and Condor with 1121 qubits. IBM is confident that this will bring it closer to the so-called "quantum advantage", the moment when quantum computers can surpass traditional systems.

This is not the limit, the development of millions of qubits of computers is already underway. They will reveal the true potential of quantum computing.

Scientific novelty. The scientific novelty of the work is the analysis of developments and inventions in the field of quantum computers, identifying issues of this type of computerization and existing solutions, analysis of the impact of this invention on living standards, and on the development of science.

Conclusions. The paper is a reflection on currently known achievements in this field of quantum computing. The innovativeness of the use of qubits as a basis for quantum mechanics is substantiated. The areas where quantum computers bring significant improvements are analyzed.

REFERENCES

1. Farzan Jazaeri, Arnout Beckers, Armin Tajalli, Jean-Michel Sallese (2019) A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics // IEEE. Available at: https://arxiv.org/pdf/1908.02656.pdf

2. James Binney, David Skinner (2008) The Physics of Quantum Mechanics // Cappella Archive. Available at https://www-thphys.physics.ox.ac.uk/people/JamesBinney/qb.pdf

3. Eleanor Rieffel, Wolfgang Polak (2011) QUANTUM COMPUTING // Massachusetts Institute of Technology. Available at http://mmrc.amss.cas.cn/tlb/201702/W020170224608150244118.pdf.

4. THE FUTURE OF QUANTUM COMPUTING // REPLY. – 2021. Available at https://trend-sonar.com/pdf/quantum_en.pdf.