UDC 004.38:530.145

QUANTUM TECHNOLOGY: QUANTUM COMPUTER

Vishnevskaya M.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Malikova I.G. – senior lecturer of the department of foreign languages

Annotation. This paper discusses the use of quantum technologies, the way of their operation and fields of application. The information provided about a quantum computer, qubits and the superposition principle will help to understand the advantages and drawbacks, possibilities and perspectives of this development.

Keywords: quantum technologies, quantum computer, qubits, superposition, photons.

Introduction. For many years, computer hardware has been getting more powerful according to Moore’ s law, which states that the amount of computing power that engineers squeeze onto a single chip appeared to double every two years. However, as electronic devices get smaller, they are reaching a limit due to quantum effects. To overcome this, we can switch to using quantum devices for computing and information processing instead of traditional electronics.

Main part. Quantum computing is based on the principles of quantum mechanics, which describe the behavior of particles at the microscopic level. A typical computer processes bits, each of which may be a «on» or «off» switch. However, quantum bits, or qubits, are the essential information-carrying parts of a quantum computer and are required to construct extremely complex entangled quantum systems. There are numerous ways to physically realize a qubit. It can be transported by a solitary atom, electron, or photon (a light particle). Alternatively, a qubit may be carried by a more complex system, such as a large number of electrons flowing in a very cold superconducting electrical circuit.

Quantum computing is considered powerful due to the unique properties of qubits, which can exist in superposition states (the ability of a particle to be in two or more states simultaneously) and be entangled with each other (the theory that changing the state of one particle can influence the behavior of another, at a distance).

The complexity of describing entangled quantum states involving many qubits surpasses the capacity of classical data representation, with the number of possible correlations among qubits exceeding the atoms in the visible universe.

There are a few explanations concerning why quantum computers perform better than traditional ones. The impossibility to simulate a quantum computer is one of them. There is currently no known classical algorithm that can faithfully copy the functions of a quantum computer, despite great efforts. This inability to simulate illustrates how quantum computing has the potential to be more powerful than traditional computer techniques. Utilizing quantum techniques to solve traditionally unsolvable issues is the second justification. Large composite integer factorization is one of the challenges that quantum algorithms have been shown to successfully deal with and that traditional computers find challenging [1].

When scientists and engineers face challenging problems, they typically rely on supercomputers, which are massive classical machines capable of executing complex calculations and advanced artificial intelligence tasks. Despite their power, supercomputers encounter limitations in solving certain types of problems.

Complex problems, characterized by many variables interacting in intricate ways, often pose a challenge for classical computers. Tasks such as modeling the behavior of individual atoms in a molecule or detecting subtle patterns of fraud in financial transactions require handling high levels of complexity. Quantum computers, leveraging the quantum states of qubits, offer a promising approach to addressing these complex problems that remain unsolvable by classical means. Given that classical computers are particularly bad at simulating the dynamics of highly entangled many-particle quantum systems, quantum computers may also have a significant edge over them in the particularly interesting field of quantum dynamics.

In essence, the real-world operations are governed by quantum physics, making quantum computers potentially the most effective tool for understanding and navigating complex phenomena in many other fields.

The advent of powerful quantum computers is expected to have a disruptive impact on current methods of privacy protection. Existing public key cryptosystems may become vulnerable to attacks by quantum computers, necessitating the development of new cryptographic techniques resistant to quantum threats. In that case, quantum randomness expansion is very helpful. Unlike deterministic classical devices, quantum devices can generate intrinsic randomness. Remarkably, this feature of quantum physics can be exploited to expand a short random seed to a much longer string of certifiably random bits. Certifiable randomness has many potential applications, for example to secure communication protocols.

Further, quantum key distribution, quantum networks, and quantum repeaters should be mentioned. Utilizing qubits, particularly photons, for generating shared encryption keys presents opportunities for secure communication. Quantum key distribution leverages the principles of quantum mechanics to prevent eavesdropping without detection. However, global distribution of quantum entanglement for key exchange remains a technological challenge.

Another field of using quantum technology is medicine, in particular quantum sensing. Quantum technology provides enhanced sensitivity and spatial resolution for certain types of sensing applications [2].

But there are some disadvantages to this development. The problem comes from a fundamental feature of the quantum world: it is impossible to observe a quantum system without creating uncontrollable disturbances within a system. This means that if we want to use quantum systems for reliable storage and information processing, we must keep this system almost completely isolated from the outside world. At the same time, we want the qubits to interact strongly with each other. so that we can process the information. We must also be able to control the external magnetic system and to read the qubits so we can find out the results of our calculations. It is very difficult to build a quantum system that satisfies all these desires and needs.

Computers use the principle of quantum error correction. The essential idea of quantum error correction, if we want to protect a quantum system from damage, is to encode it in a very entangled state; this entangled state is characterized by the environment, in interaction with each part of the system, the encrypted information cannot be seen and so it cannot be ruined. However, it costs a significant amount of money to perform quantum error correction - write protected content. Quantum information is highly entangled and requires many additional physical qubits, so it is unlikely that reliable quantum computers using quantum error correction will be available very soon [3].

Conclusion. Thus, quantum technologies can manipulate electrons, photons, and atoms to solve problems previously thought insolvable – and to open up new exiting opportunities. Quantum technologies even enable us to work with counterintuitive principles such as superposition and entanglement. Quantum technologies promise exponential speed-up, tap-proof communications, and ultra-precise and fast measurements. Such technologies can bring a huge shift in the way in which businesses solve problems dealing with optimization, mechanical simulation, and machine learning.

Quantum technologies can be more efficient than current technologies in risk management, cybersecurity, logistics, scheduling operations, discovery of medicines. This innovation has the potential to change our lives and future scientific developments. Despite the difficulty of the technology, research in this area continues, and we can expect an increasing use of quantum computers in various fields.

References

1. Quantum Computation in the NISQ era and beyond [Electronic resource]. – Mode of access: https://ar5iv.labs.arxiv.org/html/1801.00862. – Date of access: 18.03.2024.

2. What is quantum computing? [Electronic resource]. – Mode of access: https://www.ibm.com/topics/quantum-computing. – Date of access 18.03.2024.

3. Why Quantum Tech Will Change Our Future: The Day Tomorrow Began [Electronic resource]. – Mode of access: https://news.uchicago.edu/why-quantum-tech-will-change-our-future-day-tomorrow-began. – Date of access: 20.03.2024.