УДК 004.38:530.145 DOI: 10.53002/123

E.V. Kharin

Karaganda Industrial University, Temirtau, Kazakhstan
(E-mail: e.kharin@tttu.edu.kz)

The prospects for the development of quantum computers and their impact on modern science and technology

Quantum computers are one of the most interesting and promising areas of modern information technology. With their help, solving complex problems is performed several times faster than traditional computers. The development of this technology allows not only to expand the boundaries of computing, but also to revise all areas of scientific research in a new way. This article analyzes the theoretical foundations of quantum computers, the level of their development, prospects and influence on modern science and technology.

Keywords: quantum computers, quantum mechanics, quantum algorithms, superposition, encryption, quantum technologies, information security.

Introduction

Modern computing technologies operate on the basis of traditional computers, which process information using only two – value logical devices-bits. Each bit has the value "0" or "1", and they are interconnected according to certain rules to perform different operations. However, this approach works with limited capabilities and may not be effective in solving many complex problems. Quantum computers offer solutions to these problems because they are based on the laws of quantum mechanics and can have very large computing power compared to traditional computing systems.

The main feature of quantum computers is quantum bits, or qubits. Qubits can take multiple values at the same time because they are based on quantum superposition and amplification phenomena. This ability significantly increases the computational speed of quantum computers, so they can be significantly more effective than traditional computers in solving certain problems (for example, Big Data Processing, cryptography, molecular modeling).

The development of quantum computers has made several significant advances in recent years. However, they are still at the initial stage, many theoretical and technical problems require a solution. At present, the impact of quantum computers on various industries is becoming apparent, leading to major changes, including in the fields of Information Security, Artificial Intelligence, medicine and physics. In this article, we will analyze their impact on modern science and Technology, studying the development of quantum computers, current scientific and technological achievements, as well as their influence in the future.

Әдістер мен материалдар

The operating principles of quantum computers differ fundamentally from those of classical computers. While classical computing is based on classical physics and deterministic logic, quantum computing relies on the laws of quantum mechanics. To understand how quantum computers function, it is essential to become familiar with several key quantum principles.

1. Principle of Superposition: in classical computing, a bit can take only one of two values at any given time: 0 or 1. In contrast, a quantum bit, or qubit, can exist in a linear combination of both states simultaneously. This phenomenon is known as superposition.

Mathematically, a qubit can be represented as a combination of $|0\rangle$ and $|1\rangle$ states, meaning that until measurement occurs, the qubit encodes probabilities of both outcomes. Superposition enables quantum computers to process a vast number of possible solutions at once, dramatically increasing computational potential for certain classes of problems.

2. Interference: quantum systems can evolve toward a result through multiple computational paths simultaneously. These paths can interfere with one another, either reinforcing correct solutions (constructive interference) or canceling incorrect ones (destructive interference).

Interference is crucial for quantum algorithms because it allows them to amplify the probability of correct answers while suppressing incorrect possibilities. This principle is one of the main reasons why quantum algorithms can outperform classical ones for specific tasks.

3. Entanglement: qubits can become strongly correlated in a way that has no classical equivalent. This phenomenon is known as entanglement. When qubits are entangled, the state of one qubit is directly related to the state of another, regardless of the physical distance between them.

Entanglement enables highly coordinated quantum operations across multiple qubits and forms the backbone of many powerful quantum algorithms. It allows quantum computers to process complex, multidimensional information structures more efficiently than classical systems.

Table 1. Comparative Characteristics of Classical and Quantum Computers

Parameter	Classical Computer	Quantum Computer
Basic unit	Bit (0 or 1)	Qubit (0, 1, superposition)
Processing style	Sequential computations	Parallel quantum state evolution
Cryptographic impact	Difficult to break RSA	Efficient factoring via Shor’s algorithm

Today, numerous research institutions and major technology companies are actively developing quantum computing technologies. Among the most prominent organizations are IBM, Google, and Microsoft. These companies are building increasingly powerful quantum processors and refining quantum algorithms.

1. IBM and Google. In 2019, Google’s Sycamore processor achieved what was described as “quantum supremacy.” The processor completed a specific computational task in approximately 200 seconds—an operation estimated to take classical supercomputers thousands of years under similar conditions.

Although the practical implications of this demonstration remain debated, it marked a significant milestone in the development of scalable quantum hardware.

2. Medical Research Applications. Quantum computing holds substantial promise in medicine and pharmaceutical research. One of its most promising applications is molecular simulation. Accurately modeling molecular interactions is computationally expensive for classical computers, but quantum systems are naturally suited to simulate quantum mechanical behavior in chemistry.

This capability could accelerate drug discovery, protein folding analysis, and personalized medicine development.

Quantum algorithms can solve certain computational problems significantly faster than classical algorithms. The most famous example is Shor’s algorithm, introduced by Peter Shor in 1994.

Shor’s algorithm can factor large integers exponentially faster than the best-known classical algorithms. Since widely used cryptographic systems—such as RSA—rely on the computational difficulty of factoring large numbers, large-scale quantum computers could potentially break current public-key encryption schemes.

Another important quantum algorithm is Grover’s algorithm, which provides quadratic speedup for unstructured search problems. While it does not completely break symmetric encryption methods such as AES, it reduces their effective security level.

As a result, researchers are actively developing post-quantum cryptography—classical encryption methods designed to remain secure even against quantum attacks.

Despite significant progress, several major technical challenges remain:

1. Qubit instability (decoherence): Qubits are extremely sensitive to environmental disturbances.

2. Quantum error correction: Reliable error-correcting codes require many physical qubits to create one stable logical qubit.

3. Extreme cooling requirements: Many quantum processors operate at temperatures near absolute zero.

4. Scalability issues: Increasing the number of qubits while maintaining coherence remains a major engineering challenge.

If these obstacles are successfully addressed, quantum computers could revolutionize industries ranging from cybersecurity to artificial intelligence and materials science.

Нәтижелер мен пікірталас

Several companies are working toward the commercialization of quantum processors. In addition to IBM, Google, and Microsoft, companies such as Intel, IonQ, and Honeywell are developing quantum hardware and cloud-based quantum services.

The commercialization process involves not only hardware development but also software platforms, development kits, and cloud access systems that allow researchers and businesses to experiment with quantum algorithms.

Table 2. Industrial Applications of Quantum Computing

Industry	Example Applications
Medicine	Drug discovery, molecular simulation
Finance	Portfolio optimization, risk assessment
Cryptography	Quantum Key Distribution (QKD)

One of the most significant developments in quantum cryptography is Quantum Key Distribution (QKD). QKD leverages quantum mechanical principles to securely distribute encryption keys. Any attempt to intercept the key disturbs the quantum state, making eavesdropping detectable.

Unlike classical encryption methods, QKD offers theoretically provable security based on the laws of physics rather than computational complexity.

Quantum computing is reshaping educational systems worldwide. Universities are introducing specialized courses in quantum information science, quantum programming, and quantum engineering.

Developing a skilled workforce in quantum technologies requires interdisciplinary training that combines physics, computer science, mathematics, and electrical engineering. As quantum technologies mature, educational institutions must adapt their curricula to prepare the next generation of researchers and engineers.

Quantum computers are expected to play a transformative role in industries such as

1. Chemistry and pharmaceuticals: Molecular modeling and new material discovery
2. Logistics: Supply chain optimization
3. Finance: Market prediction and portfolio management
4. Artificial intelligence: Acceleration of machine learning optimization tasks

Although practical large-scale deployment is still in development, early-stage industrial experiments are already demonstrating promising results.

Conclusion

Quantum computers offer extraordinary potential for advancing science and technology. Their computational power, which can vastly exceed that of classical computers for certain tasks, enables the development of entirely new algorithms and problem-solving strategies.

However, substantial technical challenges must be overcome before quantum computing becomes fully practical and commercially widespread.

In the future, quantum computers may revolutionize information security, medicine, artificial intelligence, materials science, and many other fields. Continued research, engineering innovation, and interdisciplinary collaboration will be essential to unlocking their full potential.

References

1. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.
3. Google AI Quantum Team. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510.
4. Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature,* 574(7779), 505–510.
5. Zhou, J., et al. (2017). Quantum machine learning. *Nature*, 549(7671), 196–202.

Э.В. Харин

Кванттық компьютерлердің даму перспективалары және олардың қазіргі ғылым мен техникаға әсері

Кванттық компьютерлер-заманауи ақпараттық технологиялардың ең қызықты және перспективалы бағыттарының бірі. Олардың көмегімен күрделі мәселелерді шешу дәстүрлі компьютерлерге қарағанда бірнеше есе жылдам орындалады. Бұл технологияның дамуы есептеу техникасының шекарасын кеңейтуге ғана емес, сонымен қатар ғылыми зерттеулердің барлық салаларын жаңаша қайта қарауға мүмкіндік береді. Бұл мақалада кванттық компьютерлердің теориялық негіздері, олардың даму деңгейі, болашағы және қазіргі ғылым мен техникаға әсері талданады.

Түйінді сөздер: кванттық компьютерлер, кванттық механика, кванттық алгоритмдер, суперпозиция, шифрлау, кванттық технологиялар, ақпараттық қауіпсіздік.

Э.В. Харин

Перспективы развития квантовых компьютеров и их влияние на современную науку и технику

Квантовые компьютеры - одно из самых интересных и перспективных направлений современных информационных технологий. С их помощью решение сложных задач выполняется в несколько раз быстрее, чем на традиционных компьютерах. Развитие этой технологии позволяет не только расширить границы вычислительной техники, но и по-новому пересмотреть все направления научных исследований. В данной статье анализируются теоретические основы квантовых компьютеров, уровень их развития, перспективы и влияние на современную науку и технику.

Ключевые слова: квантовые компьютеры, квантовая механика, квантовые алгоритмы, суперпозиция, шифрование, квантовые технологии, информационная безопасность.

Список литературы

1. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.
3. Google AI Quantum Team. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510.
4. Arute, F., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510.
5. Zhou, J., et al. (2017). Quantum machine learning. *Nature*, 549(7671), 196–202.