UDC 004.382.2

QUANTUM COMPUTERS: PRINCIPLES OF OPERATION AND PROSPECTS FOR APPLICATION

Melnikov I. M., Miatselitsa M. P.

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

Perevyshko A. I. - Senior Lecturer at the Department of Foreign Languages

Annotation. This article is devoted to quantum computers. At the beginning, the reasons for their introduction are noted. Then much attention is given to the working principles of quantum computers. After that it is pointed out some examples of quantum algorithms. Next it is spoken about engineering challenges. At the end the future of quantum computing is emphasized.

Keywords: quantum computer, qubit, superposition, quantum entanglement, quantum algorithm, quantum gate.

Introduction. The growth of data volumes and computational complexity have pushed classical computers to their limits, making problems in cryptography, drug discovery, and optimisation intractable for conventional architectures. Quantum computers exploit quantum mechanical phenomena to perform calculations that would take classical supercomputers millions of years. Since Feynman proposed quantum computation in 1982 [1] and Shor demonstrated a polynomial-time factorisation algorithm in 1994 [2], the field has grown dramatically, attracting worldwide investment from governments and academia.

Main part. The fundamental unit of quantum information is the qubit (quantum bit). Unlike a classical bit, which can exist only in state 0 or 1, a qubit can exist in a superposition of both states simultaneously. Mathematically, the state of a qubit is written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex probability amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$. Upon measurement, the qubit collapses to state $|0\rangle$ with probability $|\alpha|^2$ or to $|1\rangle$ with probability $|\beta|^2$. A quantum register of n qubits can represent 2^n states simultaneously, providing an exponential increase in information space compared with classical registers [3].

A second key resource is quantum entanglement. When two or more qubits are entangled, the measurement outcome of one qubit instantaneously determines the state of its partners, regardless of the physical distance between them. Entanglement enables quantum computers to process correlated information in ways that have no classical analogue and is essential for quantum teleportation and superdense coding protocols [4].

Quantum interference is the third pillar of quantum computation. Quantum algorithms are designed so that computational paths leading to wrong answers interfere destructively (their amplitudes cancel), while paths leading to correct answers interfere constructively (their amplitudes add). This mechanism is what allows quantum algorithms to find correct answers with high probability using far fewer steps than brute-force classical search [3].

Quantum computation is most commonly described using the circuit model, which is analogous to classical Boolean circuits. Operations on qubits are performed by quantum gates – unitary transformations represented by matrices. The single-qubit Hadamard gate (H) creates an equal superposition of $|0\rangle$ and $|1\rangle$, forming the starting point of many quantum algorithms. The Pauli-X gate acts as a quantum NOT gate, flipping $|0\rangle$ to $|1\rangle$ and vice versa. The phase gate S introduces a relative phase of $\pi/2$ between the basis states [5].

Two-qubit gates enable entanglement. The Controlled-NOT (CNOT) gate flips the target qubit if and only if the control qubit is in state $|1\rangle$. Together with single-qubit rotations, the CNOT gate forms a universal set, meaning that any unitary operation on an arbitrary number of qubits can be approximated to any desired accuracy using only these elementary gates [5]. This universality is the quantum counterpart of classical NAND universality.

Shor's algorithm for integer factorisation is among the most celebrated quantum algorithms. It runs in polynomial time $O((\log N)^3)$, an exponential improvement over the best known classical algorithm, the general number field sieve [2]. Because the security of RSA encryption rests on the hardness of factorisation, a fault-tolerant quantum computer executing Shor's algorithm would render

current public-key infrastructure obsolete, motivating intensive research into post-quantum cryptography.

Grover's algorithm provides a quadratic speedup for unstructured database search, reducing the number of queries from O(N) classically to O(√N) quantumly [6]. Although a quadratic rather than exponential gain, it has broad applicability: it can accelerate any classical algorithm whose inner loop reduces to a search over N possibilities. Applications include satisfiability problems, collision finding in hash functions, and combinatorial optimisation.

The Variational Quantum Eigensolver (VQE) and the Quantum Approximate Optimisation Algorithm (QAOA) are hybrid classical-quantum algorithms designed for near-term devices. VQE estimates the ground-state energy of molecular Hamiltonians and is directly relevant to drug design and catalyst discovery; QAOA targets combinatorial optimisation problems such as portfolio balancing and traffic routing [7].

Several physical platforms are currently being explored for realising qubits. Superconducting qubits, based on Josephson junctions cooled to millikelvin temperatures, are the approach used by IBM, Google, and Rigetti. In 2019, Google's 53-qubit Sycamore processor performed a specific sampling task in 200 seconds that was estimated to require 10,000 years on the then-best classical supercomputer, a milestone described as achieving quantum computational advantage [8].

Trapped-ion systems confine individual atomic ions using electromagnetic fields and manipulate their internal electronic states with laser pulses. IonQ and Quantinuum utilise this technology, which offers higher gate fidelities and longer coherence times than superconducting qubits, albeit at slower gate speeds. Photonic qubits encode information in the quantum states of individual photons and are attractive for room-temperature operation and optical networking [9].

The primary obstacle to practical quantum computation is decoherence: unwanted interactions between qubits and their environment cause quantum states to degrade, introducing errors. Quantum error correction (QEC) codes, such as the surface code, can protect logical qubits from physical errors, but require roughly 1,000 physical qubits per logical qubit at current error rates, making large-scale fault-tolerant systems a long-term engineering challenge [10].

Despite these challenges, progress is accelerating. The NISQ (Noisy Intermediate-Scale Quantum) era, characterised by devices with 50–1,000 qubits without full error correction, is expected to demonstrate practical quantum advantage for specific industrial problems within this decade. Quantum simulation of chemical and biological systems is considered the most near-term application, promising breakthroughs in personalised medicine and the discovery of new materials for batteries and superconductors [7].

Conclusion. Quantum computers exploit superposition, entanglement, and interference to solve specific computational problems with an efficiency unattainable by classical machines. Significant engineering obstacles – chiefly decoherence and the overhead of error correction – must still be overcome before fault-tolerant quantum computing becomes a reality, yet the field is advancing rapidly. Near-term NISQ devices already offer platforms for hybrid quantum-classical algorithms with concrete applications in chemistry, optimisation, and machine learning. In the longer term, fault-tolerant quantum computers are expected to transform fields as diverse as cryptography, logistics, financial modelling, and artificial intelligence, making quantum computing one of the most strategically significant technologies of the 21st century.

References

1. Feynman R.P. Simulating physics with computers // International Journal of Theoretical Physics. – 1982. – Vol. 21. – P. 467–488.

2. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. – 1997. – Vol. 26. – P. 1484–1509.

3. Nielsen, M. A. Quantum Computation and Quantum Information/ M. A. Nielsen, I.L. Chuang – Cambridge University Press, 2010. – 704 p.

4. Einstein A., Podolsky B., Rosen N. Can quantum-mechanical description of physical reality be considered complete? // Physical Review. – 1935. – Vol. 47. – P. 777–780.

5. Barenco A. et al. Elementary gates for quantum computation // Physical Review A. – 1995. – Vol. 52. – P. 3457–3467.

6. Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings of the 28th ACM Symposium on Theory of Computing. – 1996. – P. 212–219.

7. Preskill J. Quantum computing in the NISQ era and beyond // Quantum. – 2018. – Vol. 2. – P. 79.

8. Arute F. et al. Quantum supremacy using a programmable superconducting processor // Nature. – 2019. – Vol. 574. – P. 505–510.

9. Krantz P. et al. A quantum engineer's guide to superconducting qubits // Applied Physics Reviews. – 2019. – Vol. 6. – P. 021318.

10. Fowler A.M. et al. Surface codes: Towards practical large-scale quantum computation // Physical Review A. – 2012. – Vol. 86. – P. 032324.