УДК 519.7
Наталія Маглюй, Сергій Заскалета
ННК «ІПСА», НТУУ «КПІ», Україна

КВАНТОВІ ОБЧИСЛЕННЯ

Nataliia Magliui, Sergii Zaskaleta

QUANTUM COMPUTING

Nowadays computers operate on fundamental principle formalized by Alan Turing: one stable state of the machine represents one number. Even nonstandard computation models, such as the one based on DNA, share this basic principle. Yet physicists have shown that the laws describing the natural world are not the simple laws of classical mechanics – they are the subtler laws of quantum physics. These discoveries led to the idea of using quantum principles in computing.

Quantum mechanics enables the encoding of information in quantum bits (qubits). Unlike a classical bit, which can store only a single value – either 0 or 1 – a qubit can store a one, a zero, or any quantum superposition of these. Furthermore, a quantum register of 64 qubits can store 2^{64} values at once. Quantum computers use such quantum mechanical properties of particles, as superposition and entanglement, which are responsible for most of the parallelism quantum systems achieve. As a consequence of such properties quantum algorithms offer a more than polynomial speedup over some classical algorithms.

There is an equivalent for Turing machine in quantum computing theory – Quantum Turing machine (or universal quantum computer). Any quantum algorithm can be expressed formally as a particular quantum Turing machine. Another model, which is used for analyzing quantum computation, is the quantum circuit. In this model a computation is a sequence of quantum gates, which are reversible transformations on an n-qubit register. These models are computationally equivalent.

Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers, but Shor's quantum algorithm could efficiently solve this problem. This ability would allow a quantum computer to decrypt many of the cryptographic systems in use today.

Another example of such speedup is quantum database search, which can be solved by Grover's algorithm using quadratically fewer queries to the database than are required by classical algorithms. It is proven that an equally fast classical algorithm can not exist.

Scientists predict that 10-qubit special-purpose quantum computer will be built in few years, 10-qubit general-purpose – in 10 years, and 100 qubits in 100 years.

Quantum information theory seeks to unite some of the most influential ideas of 20th-century science: quantum mechanics, computer science, and information theory. The development of quantum information theory has only begun. Where exactly the theory will lead is hard to predict, but it seems poised to contribute to some of the most exciting ideas of the 21st century. Quantum information theory gives us an ideal framework for developing a better understanding of how nature works and what it will let us do. Such advancements in knowledge led to new technologies and applications in the past and surely will do so again – to those we have suggested and to those yet undreamed of.